AVG 9.0 File Server

Руководство пользователя

Версия документа 90.7 (31. 3. 2010)

Содержимое

1. Введение 6

2. Требования для установки 7

2.1 Поддерживаемые операционные системы 7
2.2 Требования к оборудованию 7

3. Варианты установки AVG 8

4. Процесс установки AVG 9

4.1 Запуск установки 9
4.2 Лицензионное соглашение 10
4.3 Проверка состояния системы 11
4.4 Выбор типа установки 12
4.5 Активация лицензии AVG 12
4.6 Выборочная установка — Папка назначения 14
4.7 Выборочная установка — Выбор компонентов 15
4.8 AVG DataCenter 16
4.9 Установка AVG 17
4.10 Планирование регулярных сканирований и обновлений 18
4.11 Настройка защиты AVG завершена 19

5. После установки 20

5.1 Оптимизация сканирования 20
5.2 Регистрация продукта 20
5.3 Доступ к интерфейсу пользователя 20
5.4 Сканирование всего компьютера 21
5.5 Тестирование EICAR 21
5.6 Конфигурация AVG по умолчанию 22

6. Интерфейс пользователя AVG 23

6.1 Системное меню 24
6.1.1 Файл 24
6.1.2 Компоненты 24
6.1.3 История 24
6.1.4 Инструменты 24
6.1.5 Справка 24

6.2 Информация о состоянии безопасности 27
6.3 Быстрые ссылки 28
6.4 Обзор компонентов 30
6.5 Компоненты сервера 31
6.6 Статистика 32
6.7 Значок на панели задач 32

7. Компоненты AVG 34

7.1 Anti-Virus 34
7.1.1 Принципы работы Anti-Virus 34
7.1.2 Интерфейс Anti-Virus 34
7.2 Anti-Spyware 36
7.2.1 Принципы работы Anti-Spyware 36
7.2.2 Интерфейс Anti-Spyware 36
7.3 Anti-Rootkit 38
7.3.1 Принципы работы Anti-Rootkit 38
7.3.2 Интерфейс Anti-Rootkit 38
7.4 Лицензия 40
7.5 Resident Shield 41
7.5.1 Принципы работы Resident Shield 41
7.5.2 Интерфейс Resident Shield 41
7.5.3 Обнаружение Resident Shield 41
7.6 Диспетчер обновления 47
7.6.1 Принципы работы диспетчера обновления 47
7.6.2 Интерфейс диспетчера обновления 47

8. Компоненты сервера AVG 50

8.1 Documents Scanner для MS SharePoint 50
8.1.1 Принципы работы Document Scanner 50
8.1.2 Интерфейс Document Scanner 50

9. AVG для SharePoint Portal Server 52

9.1 Обслуживание программы 52
9.2 Конфигурация AVG для SPPS — SharePoint 2007 53
9.3 Конфигурация AVG для SPPS — SharePoint 2003 55

10. Расширенные параметры AVG 58

10.1 Внешний вид 58
10.2 Звуки 60

10.3 Игнорирование ошибочных условий 62
10.4 Хранилище вирусов 63
10.5 Исключения PUP 64
10.6 Сканирования 67
10.6.1 Сканирование всего компьютера 67
10.6.2 Сканирование расширения оболочки 67
10.6.3 Сканирование отдельных файлов или папок 67
10.6.4 Сканирование съемного устройства 67
10.7 Расписания 74
10.7.1 Запланированное сканирование 74
10.7.2 Расписание обновления вирусной базы данных 74
10.7.3 Расписание обновления программы 74
10.8 Resident Shield 85
10.8.1 Дополнительные параметры 85
10.8.2 Исключаемые каталоги 85
10.8.3 Исключенные файлы 85
10.9 Сервер кэширования 91
10.10 Anti-Rootkit 93
10.11 Обновление 94
10.11.1 Прокси-сервер 94
10.11.2 Подключение по коммутируемой линии 94
10.11.3 URL-адрес 94
10.11.4 Управление 94
10.12 Удаленное администрирование 102
10.13 Компоненты сервера 103
10.13.1 Document Scanner для MS SharePoint 103

11. Сканирование AVG 108

11.1 Интерфейс сканирования 108
11.2 Предопределенные сканирования 109
11.2.1 Сканирование всего компьютера 109
11.2.2 Сканирование отдельных файлов или папок 109
11.2.3 Сканирование Anti-Rootkit 109
11.3 Сканирование в Проводнике Windows 119
11.4 Сканирование с помощью командной строки 120
11.4.1 Параметры сканирования с помощью командной строки 120
11.5 Расписание сканирования 123
11.5.1 Параметры расписания 123

11.5.2 Способы сканирования *123*
11.5.3 Объекты сканирования *123*
11.6 Обзор результатов сканирования 133
11.7 Сведения о результатах сканирования 135
11.7.1 Вкладка "Обзор результатов" *135*
11.7.2 Вкладка "Заражения" *135*
11.7.3 Вкладка "Шпионское ПО" *135*
11.7.4 Вкладка "Предупреждения" *135*
11.7.5 Вкладка Rootkits *135*
11.7.6 Вкладка "Сведения" *135*
11.8 Хранилище вирусов 145

12. Обновления AVG 147

12.1 Уровни обновлений 147
12.2 Типы обновлений 147
12.3 Процесс обновления 147

13. Журнал событий 149

14. Диспетчер параметров AVG 151

15. Часто задаваемые вопросы и техническая поддержка 154

1. Введение

Руководство пользователя содержит полные сведения о системе **AVG 9.0 File Server**.

Поздравляем с приобретением AVG 9.0 File Server!

AVG 9.0 File Server является одним из представителей линейки продуктов AVG, удостоенных различных наград, который создан для обеспечения вашего спокойствия и полной безопасности компьютера. Как и другие продукты, система **AVG 9.0 File Server** была полностью переработана для обеспечения традиционно высокой безопасности продуктов AVG, а также имеет новый, более удобный и эффективный интерфейс.

Новый продукт **AVG 9.0 File Server** имеет улучшенный интерфейс, а также более эффективные и быстрые возможности сканирования. Для удобства пользователей многие функции были автоматизированы. Кроме того, в программу были включены интеллектуальные пользовательские параметры, позволяющие настроить функции безопасности в соответствии с потребностями пользователя. Вам больше не потребуется выбирать между удобством и безопасностью!

Программа AVG разработана и предназначена для обеспечения безопасности во время работы за компьютером и в Интернете. Благодаря AVG вы будете получать удовольствие от работы за полностью защищенным компьютером.

2. Требования для установки

2.1. Поддерживаемые операционные системы

AVG 9.0 File Server обеспечивает защиту рабочих станций, на которых используются следующие операционные системы.

- Windows 2000 Server
- Windows 2003 Server и Windows 2003 Server x64 Edition
- Windows 2008 Server и Windows 2008 Server x64 Edition

(И, возможно, более поздние пакеты обновления для некоторых операционных систем.)

2.2. Требования к оборудованию

Минимальные требования к оборудованию для **AVG 9.0 File Server**.

- Процессор Intel Pentium 1,5 ГГц.
- 470 МБ свободного места на жестком диске (для установки).
- 512 МБ памяти ОЗУ.

Рекомендуемые требования к оборудованию для **AVG 9.0 File Server**.

- Процессор Intel Pentium 1,8 ГГц.
- 600 МБ свободного места на жестком диске (для установки).
- 512 МБ памяти ОЗУ.

3. Варианты установки AVG

Программу AVG можно установить с помощью соответствующего файла на установочном компакт-диске или, загрузив последнюю версию программы на веб-сайте AVG (http://www.avg.com).

Перед началом установки программы AVG настоятельно рекомендуется посетить веб-сайт AVG (http://www.avg.com), чтобы проверить наличие нового файла установки. Это обеспечит установку последней версии AVG 9.0 File Server.

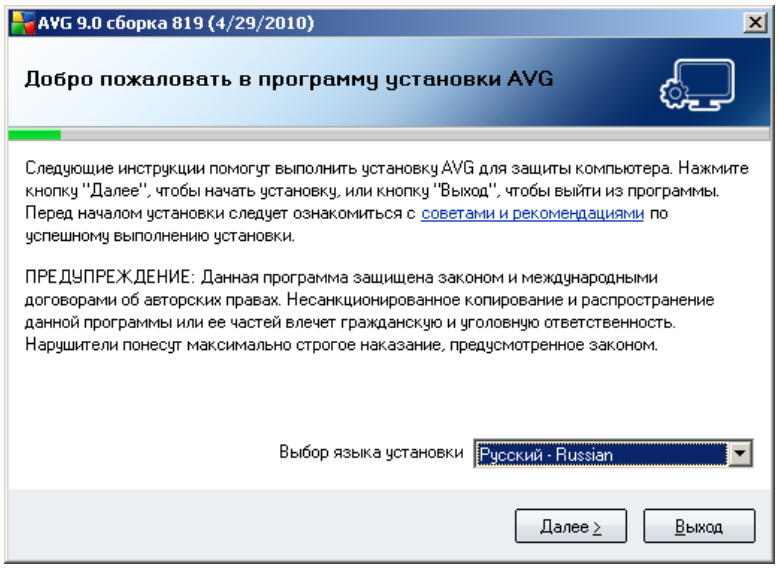
В процессе установки отобразится запрос на ввод номера лицензии или продажи. Убедитесь в наличии этих номеров перед началом установки. Номер продажи см. на упаковке компакт-диска. При покупке программы AVG в Интернете номер лицензии предоставляется пользователю по электронной почте.

4. Процесс установки AVG

Для установки **AVG 9.0 File Server** на компьютер требуется файл установки последней версии. Можно использовать файл установки на компакт-диске, включенном в коробочную версию, но этот файл может устареть. Поэтому рекомендуется загружать последние файлы установки в Интернете. Файл можно загрузить с веб-сайта компании AVG (http://www.avg.com) в разделе ***Загрузка***.

Установка — это последовательность диалоговых окон с кратким описанием необходимых действий на каждом этапе. Далее приводится описание каждого диалогового окна.

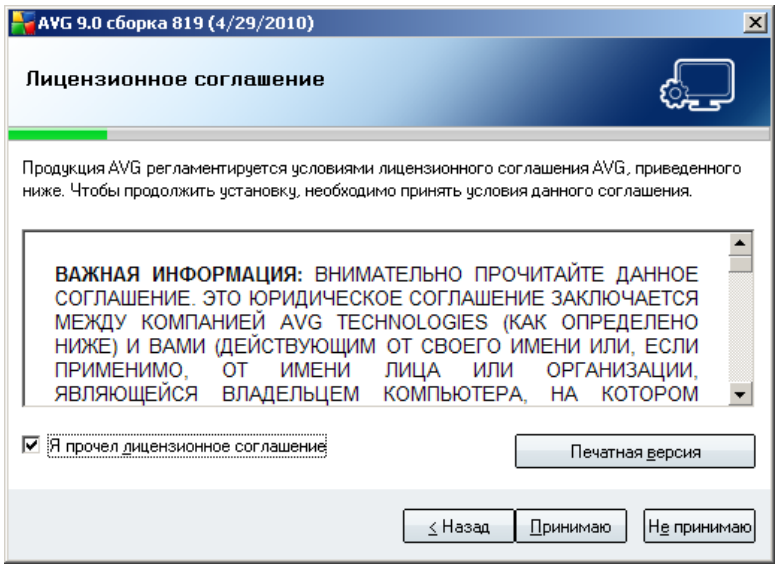
4.1. Запуск установки



Процесс установки начинается с открытия окна ***Вас приветствует программа установки AVG***. В данном окне необходимо выбрать язык, который будет использоваться во время процесса установки. В нижней части диалогового окна найдите элемент ***Выбор языка установки*** и выберите в раскрывающемся меню необходимый язык. Затем нажмите кнопку ***Далее*** , чтобы подтвердить выбор и перейти к следующему диалоговому окну.

Внимание! *Язык, выбранный в начале процесса установки, будет использоваться в приложении AVG. Однако позже его можно будет легко изменить. В интерфейсе пользователя AVG выберите Инструменты -> Дополнительные параметры -> Внешний вид).*

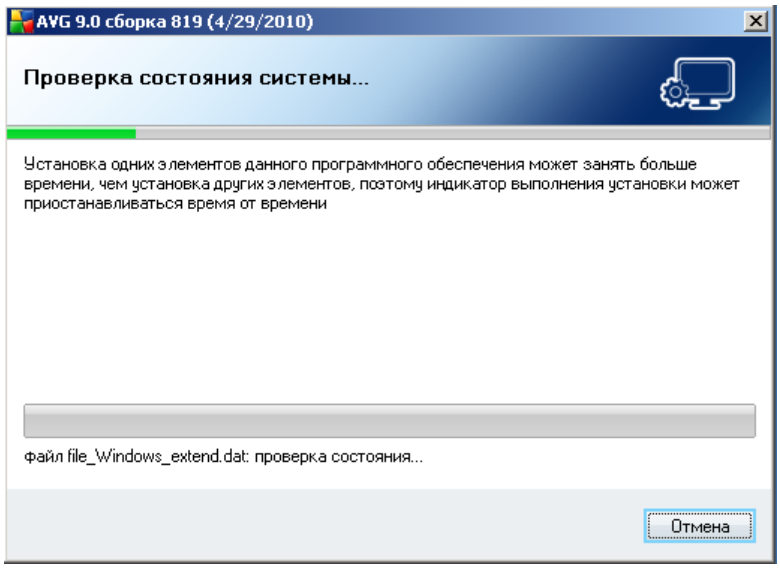
4.2. Лицензионное соглашение



Диалоговое окно ***Лицензионное соглашение*** содержит полную версию лицензионного соглашения AVG. Прочитайте его внимательно и подтвердите, что вы прочитали, понимаете и принимаете соглашение, установив флажок ***Я прочитал лицензионное соглашение*** и нажав кнопку ***Принять***.

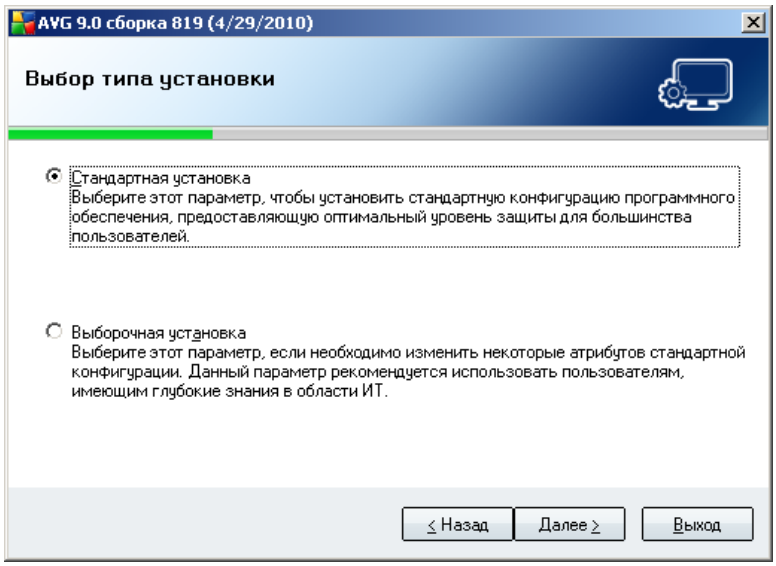
Если вы не согласны с лицензионным соглашением, нажмите кнопку ***Не принимать***. Процесс установки будет немедленно прерван.

4.3. Проверка состояния системы



После подтверждения пользовательского соглашения вы будете перенаправлены в диалоговое окно ***Проверка состояния системы***. Данное диалоговое окно не требует от пользователя никаких действий. Перед началом установки AVG будет выполнена проверка системы. Дождитесь завершения процесса, после чего вы будете автоматически перенаправлены в следующее диалоговое окно.

4.4. Выбор типа установки



Диалоговое окно ***Выбор типа установки*** позволяет выбрать один из двух вариантов установки: ***стандартная*** и ***выборочная*** установка.

Для большинства пользователей рекомендуется выбирать ***стандартную установку***, которая выполняется полностью в автоматическом режиме, устанавливая AVG с настройками, предварительно заданными поставщиком программного обеспечения. Данный вариант установки обеспечивает максимальный уровень защиты наряду с оптимальным уровнем использования ресурсов. Если в дальнейшем потребуется изменить конфигурацию, это всегда можно будет сделать напрямую в приложении AVG.

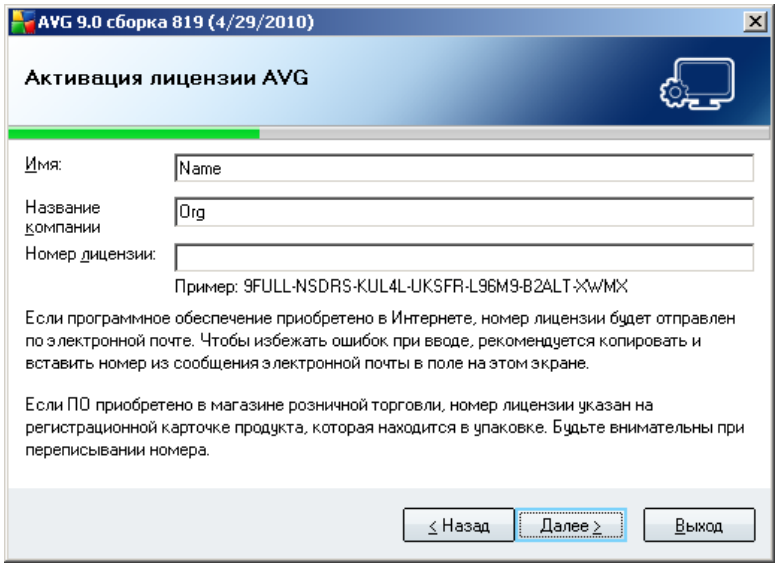
Выборочную установку следует использовать только опытным пользователям, у которых есть значительные основания для установки приложения AVG с параметрами, отличными от стандартных (например, при наличии специальных системных требований).

4.5. Активация лицензии AVG

В диалоговом окне ***Активация лицензии AVG*** необходимо указать регистрационные сведения. Введите свое имя (в поле ***Имя пользователя***) и название организации (в поле ***Название компании***).

Затем введите номер лицензии или номер продажи в текстовое поле ***Номер лицензии***. Номер продажи указан на футляре компакт-диска в коробке **AVG 9.0**

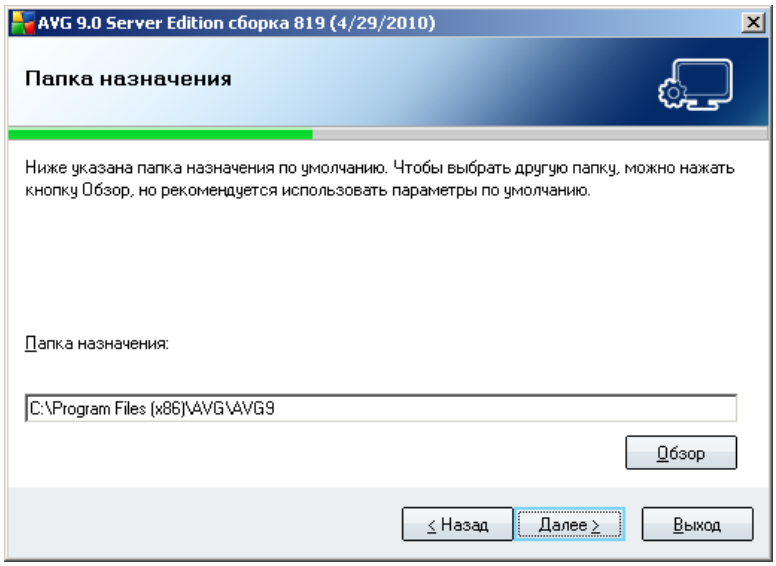
File Server. Номер лицензии будет указан в подтверждающем сообщении электронной почты, которое будет получено после оформления покупки **AVG 9.0 File Server** через Интернет. Необходимо правильно ввести номер. Номер лицензии в цифровом виде (*приведенный в сообщении электронной почты*) можно вставить с использованием стандартного метода копирования и вставки.



Чтобы продолжить процесс установки, нажмите кнопку ***Далее***.

Если на предыдущем шаге была выбрана стандартная установка, то автоматически произойдет переход к диалоговому окну ***Установка AVG***. Если была выбрана выборочная установка, откроется диалоговое окно ***Папка назначения***.

4.6. Выборочная установка — Папка назначения

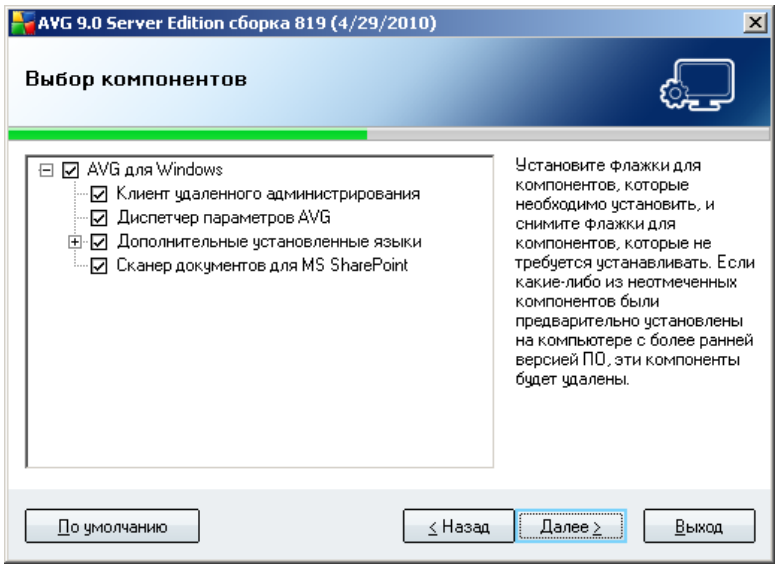


В диалоговом окне ***Папка назначения*** можно выбрать папку, в которую будет установлена система **AVG 9.0 File Server**. По умолчанию установка AVG выполняется в папку Program Files, которая расположена на диске C:. Если папка еще не существует, в новом диалогов окне будет предложено подтвердить создание новой папки для AVG.

Чтобы изменить это местоположение, используйте кнопку ***Обзор***, после нажатия которой отобразится структура дисков, в которой можно выбрать соответствующую папку.

Для подтверждения нажмите кнопку ***Далее***.

4.7. Выборочная установка — Выбор компонентов



Диалоговое окно ***Выбор компонентов*** содержит обзор всех компонентов **AVG 9.0 File Server**, которые могут быть установлены. Если значения параметров по умолчанию не подходят, можно добавить или удалить определенные компоненты.

- ***Выбор языка***

  В списке устанавливаемых компонентов можно указать язык (или несколько языков), который будет использоваться при установке AVG. Установите флажок ***Дополнительные установленные языки***, а затем выберите необходимые языки в соответствующем меню.

- ***Удаленное администрирование***

  Если необходимо позже подключить компьютер к системе удаленного администрирования AVG, отметьте флажком соответствующий элемент для установки.

- ***Диспетчер параметров AVG***

  Диспетчер параметров AVG — это небольшое приложение, позволяющее легко и быстро настраивать локальные параметры (даже те, которые не работают под управлением компонента Удаленное администрирование). Данное приложение использует файлы конфигурации (в формате PCK). Эти файлы можно легко создать с помощью Диспетчера параметров AVG на

каждом компьютере с установленным приложением AVG. Затем эти файлы можно копировать на любое съемное устройство и использовать на каждом компьютере. Данные действия также применимы непосредственно к Диспетчеру параметров AVG. Для получения дополнительной информации об этом приложении щелкните **здесь**.

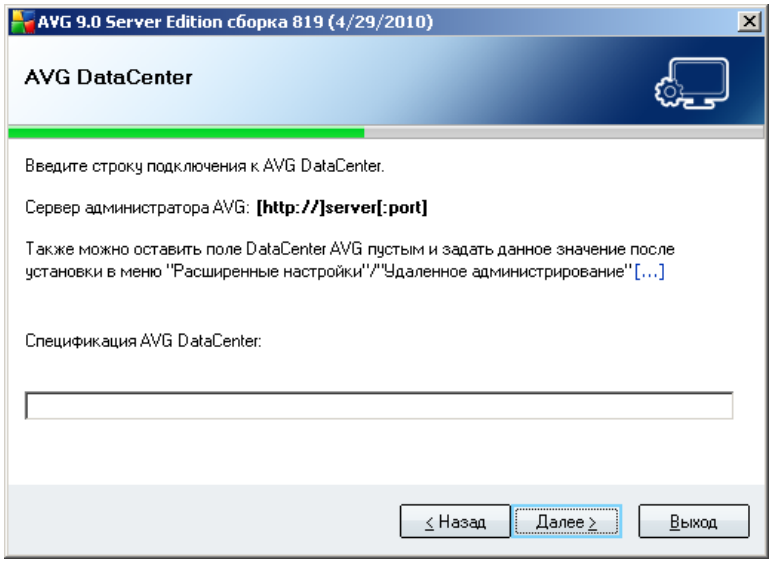
- ***Document Scanner для MS SharePoint***

  Этот компонент сканирует файлы документов, хранящиеся в MS SharePoint, и обеспечивает защиту от возможных угроз. Этот компонент является важной частью системы **AVG 9.0 File Server**, и мы настоятельно рекомендуем установить его.

Чтобы продолжить, нажмите кнопку ***Далее***.

4.8. AVG DataCenter

Если используется сетевая лицензия AVG и в предыдущем диалоговом окне ***Выборочная установка — Выбор компонентов*** была выбрана установка компонента ***Удаленное администрирование***, необходимо указать параметры ***AVG DataCenter***.



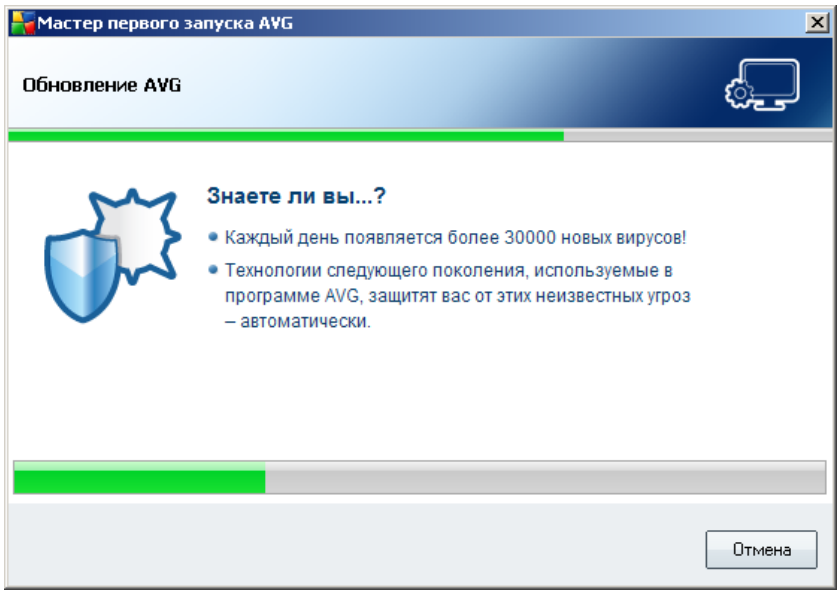
В текстовом поле ***Спецификация AVG DataCenter*** укажите строку подключения для ***AVG DataCenter*** в виде *сервер:порт*. Если в настоящий момент эта информация недоступна, оставьте поле незаполненным. Установить конфигурацию можно позже с помощью диалогового окна ***Дополнительные***

параметры/Удаленное администрирование.

Примечание. *Для получения дополнительных сведений об удаленном администрировании AVG обратитесь к руководству пользователя сетевой версии AVG, которое можно загрузить с веб-сайта AVG (http://www.avg.com).*

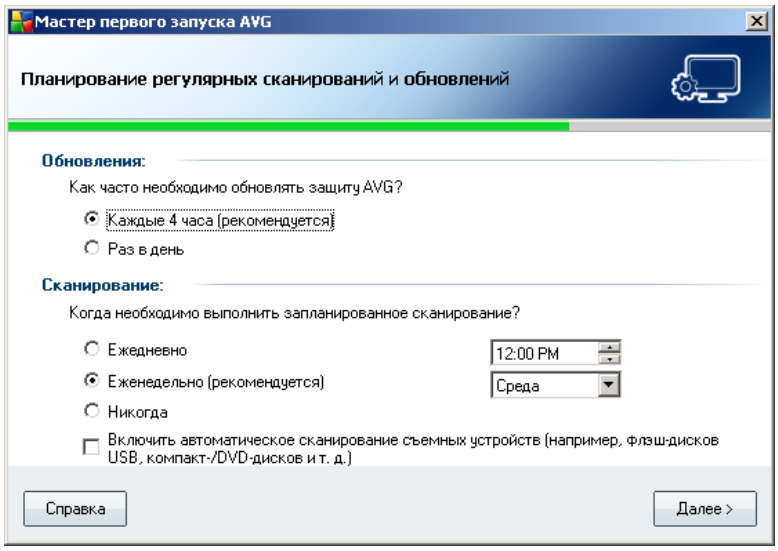
4.9. Установка AVG

В диалоговом окне ***Установка AVG*** отображается ход выполнения процесса установки. Данное окно не требует от пользователя каких-либо действий.



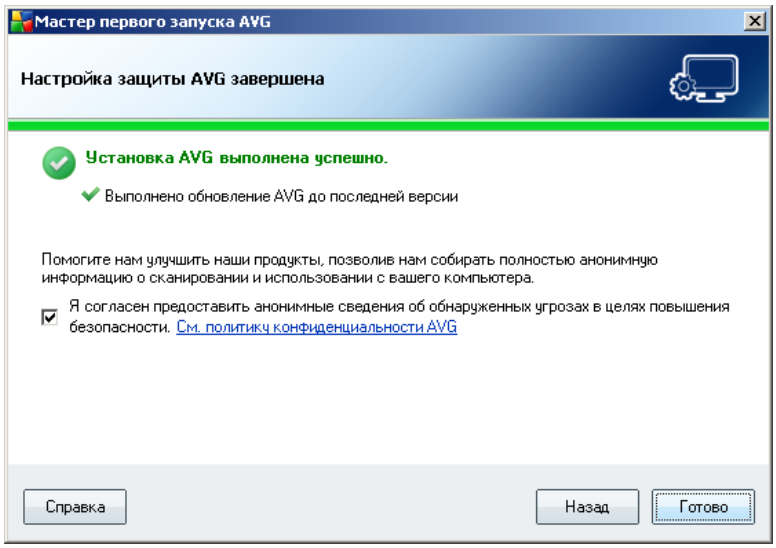
После завершения процесса установки переход к следующему диалоговому окну будет произведен автоматически.

4.10. Планирование регулярных сканирований и обновлений



В диалоговом окне ***Планирование регулярных сканирований и обновлений*** необходимо установить временной интервал проверки доступности новых файлов обновлений, а также определить время запуска запланированного сканирования. Рекомендуется оставить значения по умолчанию. Нажмите кнопку ***Далее***, чтобы продолжить.

4.11. Настройка защиты AVG завершена



Теперь система **AVG 9.0 File Server** настроена.

В данном окне можно включить или отключить функцию анонимного предоставления отчетов об эксплойтах и вредоносных сайтах в вирусную лабораторию AVG. Чтобы включить функцию, установите флажок ***Я согласен предоставлять АНОНИМНЫЕ сведения об обнаруженных угрозах с целью повышения безопасности***.

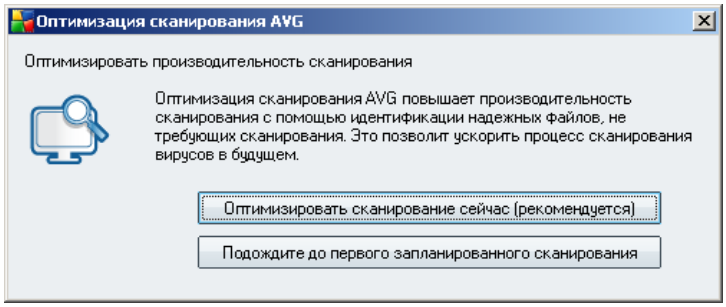
Затем нажмите кнопку ***Готово***.

5. После установки

5.1. Оптимизация сканирования

Функция оптимизации сканирования выполняет поиск в папках *Windows* и *Program files*. Она определяет соответствующие файлы в этих папках (*в данный момент такие файлы имеют расширения *.exe, *.dll и *.sys*) и сохраняет сведения о них. В следующий раз такие файлы не будут сканироваться, что значительно уменьшит время выполнения процедуры сканирования.

После завершения процесса установки в новом окне отобразится приглашение на оптимизацию сканирования.



Рекомендуется использовать эту функцию и запустить процесс оптимизации сканирования с помощью кнопки ***Оптимизировать сканирование сейчас***.

5.2. Регистрация продукта

После завершения установки **AVG 9.0 File Server** выполните регистрацию продукта через Интернет на веб-сайте AVG (http://www.avg.com) на странице ***Регистрация*** (*следуйте инструкциям на странице*). После регистрации вы получите полный доступ к учетной записи пользователя AVG, информационному бюллетеню обновлений AVG, а также к другим службам, доступ к которым имеют только зарегистрированные пользователи.

5.3. Доступ к интерфейсу пользователя

Доступ к ***Интерфейсу пользователя AVG*** можно получить одним из следующих способов:

- с помощью двойного щелчка значка AVG на панели задач

- с помощью двойного щелчка значка AVG на рабочем столе
- с помощью меню ***Пуск/Все программы/AVG 9.0/Интерфейс пользователя AVG***

5.4. Сканирование всего компьютера

Существует потенциальная опасность того, что до установки **AVG 9.0 File Server** компьютер был заражен вирусом. Поэтому необходимо запустить ***сканирование всего компьютера***, чтобы убедиться, что компьютер не заражен.

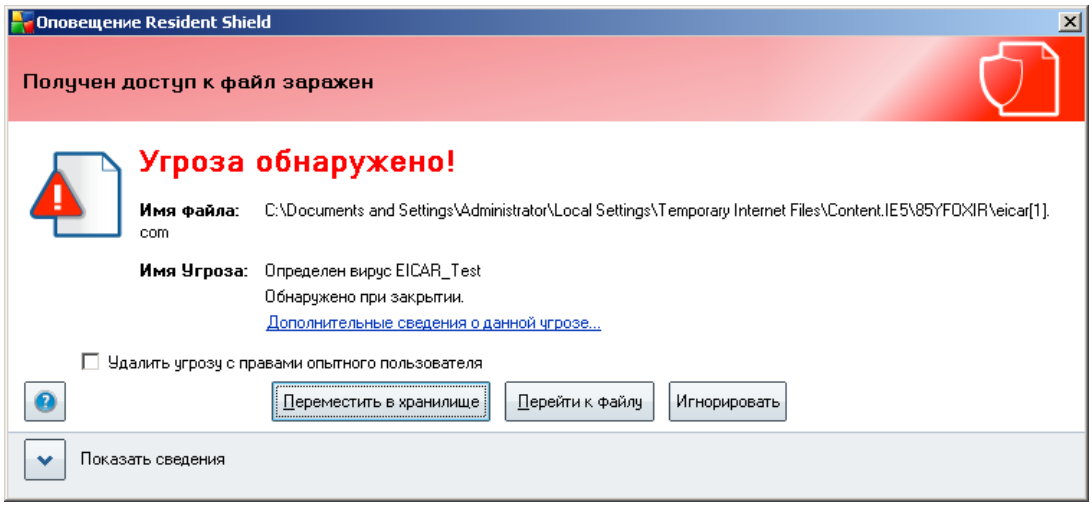
Инструкции по запуску ***сканирования всего компьютера*** см. в главе ***Сканирование AVG***.

5.5. Тестирование EICAR

Чтобы проверить правильность установки **AVG 9.0 File Server**, можно выполнить тест EICAR.

Тестирование EICAR — стандартный и абсолютно безопасный метод для тестирования работы антивирусных систем. Оно безопасно, так как не является настоящим вирусом и не включает в себя фрагментов вирусного кода. Большинство продуктов реагируют на него как на настоящий вирус (*хотя они обычно сообщают о нем, используя настоящее имя, например "EICAR-AV-Test"*). Загрузить вирус EICAR можно на веб-сайте EICAR www.eicar.com; также там можно получить необходимую информацию о проверке EICAR.

Загрузите файл ***eicar.com*** и сохраните его на локальном диске. Сразу после подтверждения загрузки тестового файла ***Resident Shield отреагирует предупреждением.*** Данное оповещение ***Resident Shield*** означает, что AVG на компьютере установлен правильно.



Если AVG не удалось определить тестовый файл EICAR как вирус, проверьте параметры программы еще раз.

5.6. Конфигурация AVG по умолчанию

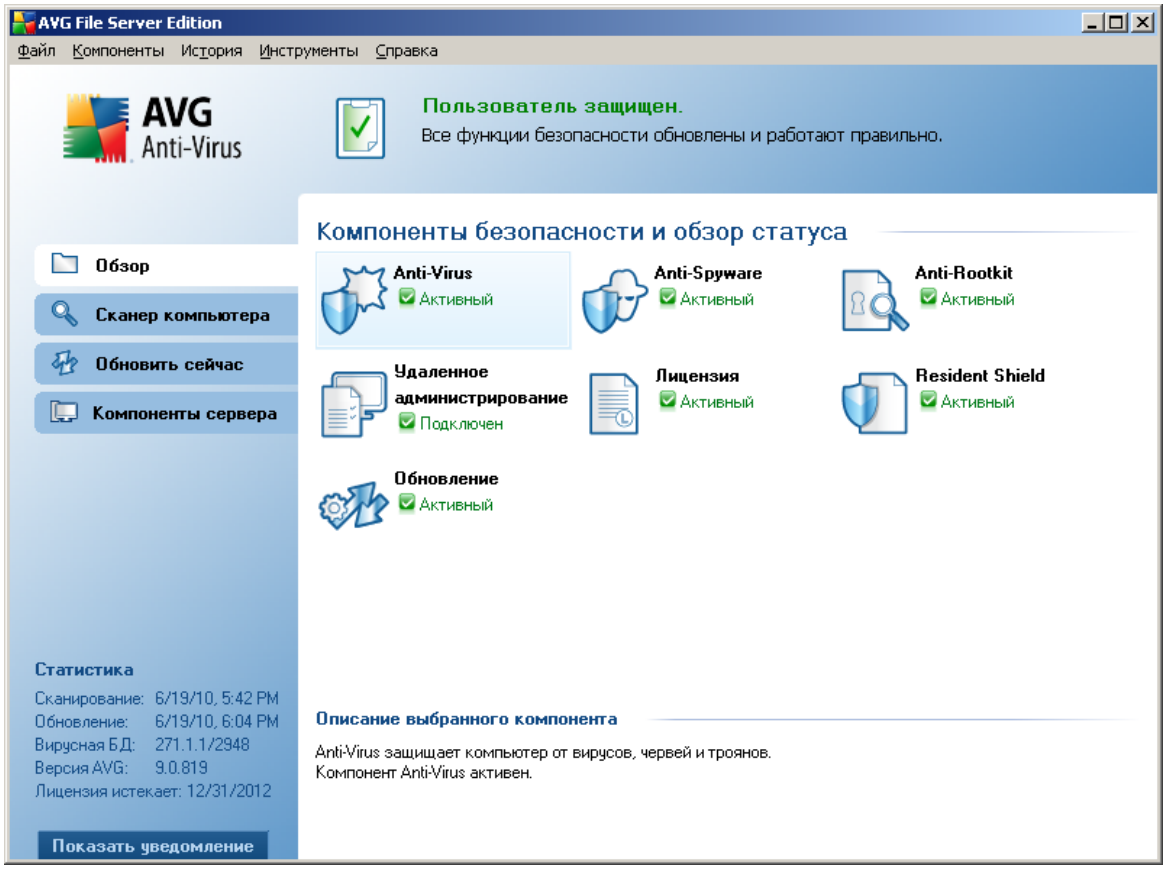
Параметры по умолчанию (*параметры приложения после установки*) **AVG 9.0 File Server** настроены поставщиком ПО таким образом, чтобы все компоненты и функции обеспечивали оптимальную производительность.

Не изменяйте настройки AVG без необходимости! Все изменения параметров должны выполняться опытным пользователем.

Допустимо незначительное изменение параметров компонентов AVG непосредственно с помощью интерфейса пользователя определенного компонента. Чтобы при необходимости изменить параметры AVG, используйте диалоговое окно ***Дополнительные параметры AVG***: выберите элемент системного меню ***Инструменты/Дополнительные параметры*** и измените параметры AVG в отобразившемся диалоговом окне ***Расширенные настройки AVG***.

6. Интерфейс пользователя AVG

AVG 9.0 File Server открывается в главном окне.



Главное окно состоит из нескольких разделов.

- ***Системное меню*** *(системная область в верхней части окна)* — это стандартное средство навигации, с помощью которого можно получить доступ ко всем компонентам, службам и функциям. Подробные сведения >>
- ***Информация о состоянии безопасности*** *(верхняя часть окна)*. Информация о текущем состоянии программы AVG. Подробные сведения >>
- ***Быстрые ссылки*** *(левая часть окна)*. Позволяет получить быстрый доступ к наиболее важным и часто используемым задачам AVG. Подробные сведения >>

- ***Обзор компонентов*** *(центральная часть окна)*. Обзор всех установленных компонентов. Подробные сведения >>

- ***Статистика*** *(левая нижняя часть окна)*. Статистическая информация о работе программы. Подробные сведения >>

- ***Значок на панели задач*** *(правая нижняя часть экрана, панель задач).* Отображение текущего состояния AVG. Подробные сведения >>

6.1. Системное меню

Системное меню — это стандартное средство навигации, которое используется во всех приложениях Windows. Оно расположено горизонтально в верхней части главного окна **AVG 9.0 File Server**. С помощью системного меню можно получить доступ к специальным компонентам, службам и функциям AVG.

Системное меню состоит их двух основных разделов.

6.1.1. Файл

- ***Выход***. Закрытие интерфейса **AVG 9.0 File Server**пользователя. При нажатии данной кнопки приложение AVG продолжит свою работу в фоновом режиме, а компьютер будет находиться под защитой!

6.1.2. Компоненты

Элемент ***Компоненты*** системного меню содержит ссылки на все установленные компоненты AVG и позволяет открывать их стандартные диалоговые окна в интерфейсе пользователя.

- ***Обзор системы***. Переключение к стандартному диалоговому окну интерфейса пользователя, которое содержит обзор всех установленных компонентов и сведения об их состоянии.

- ***Компоненты сервера***. Переключение к стандартному диалоговому окну интерфейса пользователя, которое содержит обзор всех установленных компонентов сервера и сведения об их состоянии.

- ***Anti-Virus***. Открытие стандартной страницы компонента ***Anti-Virus***.

- ***Anti-Rootkit***. Открытие стандартной страницы компонента ***Anti-Rootkit***.

- ***Anti-Spyware***. Открытие стандартной страницы компонента ***Anti-Spyware***

- ***Удаленное администрирование***. Открытие стандартной страницы

компонента ***Удаленное администрирование*** (данный компонент связывает экземпляр программы AVG с программой Удаленное администрирование AVG, что позволит сетевому администратору запускать определенные действия приложения удаленно). Компонент Удаленное администрирование будет доступен, только если он был выбран на шаге ***Выбор компонентов*** в ***процессе установки***).

- ***SharePoint***. Открытие стандартной страницы компонента сервера ***сканирования документа для MS SharePoint***.
- ***Лицензия***. Открытие стандартной страницы компонента ***Лицензия***.
- ***Resident Shield***. Открытие стандартной страницы компонента ***Resident Shield***.
- ***Диспетчер обновления***. Открытие стандартной страницы компонента ***Диспетчер обновления***.

6.1.3. История

- ***Результаты сканирования***. Переход в интерфейс проверки AVG в диалоговое окно ***Обзор результатов сканирования***.
- ***Обнаружение Resident Shield*** — отображение диалогового окна с обзором угроз, обнаруженных компонентом ***Resident Shield***
- ***Хранилище вирусов***. Отображение интерфейса среды карантина (***хранилища вирусов***), куда программа AVG отправляет все обнаруженные зараженные файлы, которые по какой-либо причине не удалось вылечить автоматически. Внутри зоны карантина зараженные файлы изолированы и не представляют угрозы для безопасности компьютера, но в то же время они сохраняются для их возможного восстановления в будущем.
- ***Журнал событий***. Отображение интерфейса журнала событий с обзором всех зарегистрированных в журнале действий **AVG 9.0 File Server**.

6.1.4. Инструменты

- ***Сканировать компьютер***. Переход к интерфейсу сканирования AVG и запуск сканирования всего компьютера.
- ***Сканировать выбранную папку***. Переход к интерфейсу сканирования AVG, который позволяет с помощью структуры дерева определить, какие файлы и папки должны быть сканированы.

- ***Сканировать файл***. Позволяет запустить проверку по требованию отдельного файла, выбранного в древовидной структуре диска.

- ***Обновить***. Автоматический запуск процесса обновления **AVG 9.0 File Server**

- ***Обновить из каталога***. Запуск процесса обновления с помощью файлов обновления, расположенных в указанной папке на локальном диске. Однако данный параметр рекомендуется использовать только в экстренном случае. Например, в случае отсутствия подключения к Интернету (*например, компьютер заражен и отключен от Интернета или подключен к сети, не имеющей доступа к Интернету и т. п.*). В открывшемся окне выберите папку, в которой ранее был размещен файл обновления, и запустите процесс обновления.

- ***Дополнительные параметры***. Открытие диалогового окна ***Дополнительные параметры AVG***, которое позволяет изменять параметры программы **AVG 9.0 File Server**. В основном, рекомендуется не изменять стандартные параметры приложения, определенные производителем.

6.1.5. Справка

- ***Содержание***. Открытие файла справки AVG.

- ***Интерактивная справка***. Открытие веб-сайта AVG (http://www.avg.com) на странице центра поддержки пользователей.

- ***AVG Web***. Открытие веб-сайта AVG (http://www.avg.com).

- ***О вирусах и угрозах***. Открытие интерактивной ***энциклопедии вирусов***, в которой можно найти подробные сведения об обнаруженных вирусах.

- ***Загрузить AVG Rescue CD***. Открытие интернет-браузера и переход на страницу ***Центр поддержки/Загрузка*** веб-сайта AVG. Введите номер лицензии в текстовое поле, чтобы загрузить последнюю версию AVG Rescue CD (*портативная версия системы AVG, предназначенная для восстановления операционной системы в таких ситуациях, когда систему нельзя загрузить обычным образом, например при большом количестве заражений вирусами*).

- ***Повторно активировать***. Открытие диалогового окна ***Активировать AVG*** с данными, введенными в диалоговом окне ***Персонализация AVG*** при установке. В данном диалоговом окне можно ввести номер лицензии, чтобы заменить им номер продажи (*номер, который использовался при установке*

AVG) или заменить старый номер лицензии (*например, при обновлении до нового продукта AVG*).

- ***Регистрация***. Переход на страницу регистрации веб-сайта AVG (http://www.avg.com). Введите данные для регистрации. Только клиенты, зарегистрировавшие продукт AVG, могут получать бесплатную техническую поддержку.

- ***О программе AVG***. Открытие диалогового окна ***Сведения***, содержащего пять вкладок, на которых представлены данные о названии программы, версии программы и вирусной базы данных, системная информация, лицензионное соглашение, а также контактная информация компании ***AVG Technologies CZ***.

6.2. Информация о состоянии безопасности

Раздел ***Информация о состоянии безопасности*** расположен в верхней части главного окна AVG. Этот раздел позволяет быстро определить текущее состояние безопасности **AVG 9.0 File Server**. Ознакомьтесь со значками, представленными в данном разделе, и их значением.

 Зеленый значок означает, что программа AVG работает правильно. Компьютер полностью защищен, установлены все необходимые обновления. Все установленные компоненты также работаю правильно.

 Оранжевый значок означает, что один или несколько компонентов настроены неправильно. Необходимо обратить внимание на их свойства или параметры. Никаких серьезных проблем, связанных с работой AVG, нет. Скорее всего, некоторые компоненты были отключены по какой-либо причине. Программа AVG также продолжает обеспечивать защиту компьютера. Однако необходимо уделить внимание настройке компонента. Его имя будет отображено в разделе ***Информация о состоянии безопасности***.

Данный значок отображается также в том случае, если по какой-либо причине было принято решение игнорировать состояние ошибки компонента (*параметр "Игнорировать состояние компонента" доступен в контекстном меню, отображаемом при нажатии с помощью правой кнопки мыши значка соответствующего компонента в обзоре компонентов в главном окне AVG*). Данный параметр может потребоваться в определенной ситуации, но

настоятельно рекомендуется отключать параметр ***Игнорировать состояние компонента*** при отсутствии необходимости использовать его.

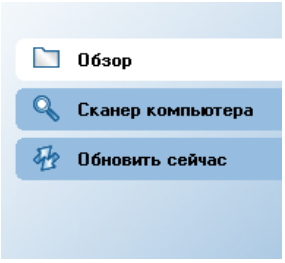
 Красный значок означает критическое состояние AVG. Один или несколько компонентов работают неправильно, программа AVG не может защитить компьютер. Необходимо немедленно устранить указанные проблемы. Если проблему не удается устранить самостоятельно, обратитесь в службу технической поддержки AVG.

Настоятельно рекомендуется обращать внимание на раздел ***Информация о состоянии безопасности***. В случае возникновения проблемы необходимо постараться незамедлительно ее устранить. В противном случае безопасность компьютера может быть под угрозой.

Примечание. *Информация о состоянии безопасности может быть получена в любое время с помощью значка на панели задач.*

6.3. Быстрые ссылки

Быстрые ссылки *(в левой части интерфейса пользователя AVG)* позволяют получить быстрый доступ к наиболее важным и часто используемым функциям AVG.



- ***Обзор*** . Используйте данную ссылку для переключения с открытого в настоящее время интерфейса AVG к стандартному интерфейсу, содержащему обзор всех установленных компонентов — см. ***Обзор компонентов >>***

- ***Сканер компьютера***. Используйте данную ссылку для открытия интерфейса сканирования AVG, с помощью которого можно напрямую запускать проверки, запланированные сканирования или изменять их параметры — см. ***Сканирование AVG >>***

- ***Обновить сейчас***. Данная ссылка открывает интерфейс обновления и немедленно запускает процесс обновления AVG — см. ***Обновления AVG >>***

- ***Компоненты сервера***. Используйте данную ссылку для переключения с открытого в настоящее время интерфейса AVG к стандартному интерфейсу, содержащему обзор компонентов сервера — см. ***Компоненты сервера >>***

Данные ссылки всегда доступны в интерфейсе пользователя. После выбора ссылки для запуска определенного процесса графический интерфейс пользователя переключится к новому диалоговому окну, но быстрые ссылки будут по-прежнему доступны.

6.4. Обзор компонентов

Раздел ***Обзор компонентов*** расположен в центральной части интерфейса пользователя AVG. Раздел состоит из двух частей.

- Обзор всех установленных компонентов, состоящих из панели со значком компонента и информации об активности компонента.
- Описание выбранного компонента

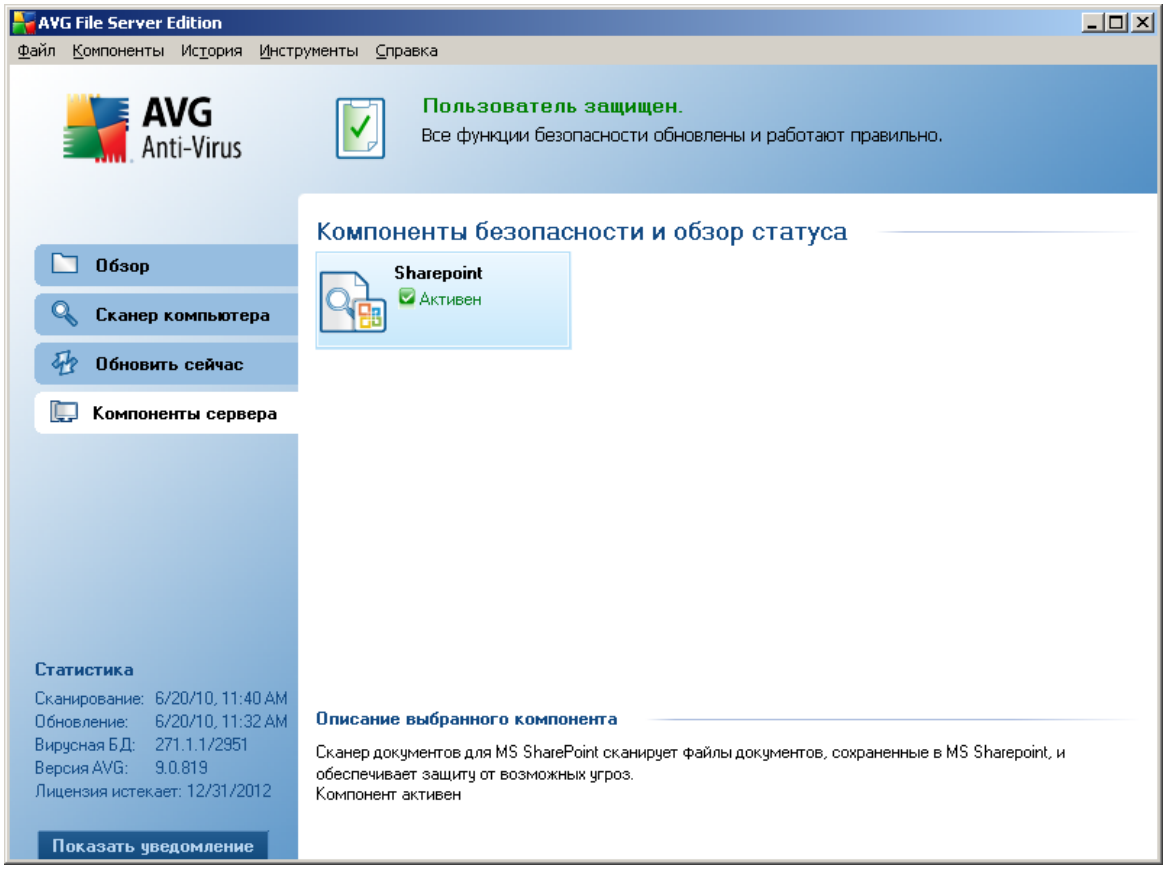
В **AVG 9.0 File Server** раздел ***Обзор компонентов*** содержит сведения о следующих компонентах.

- ***Anti-Virus***. Обеспечивает защиту от вирусов, проникающих на компьютер. Подробные сведения >>
- ***Anti-Spyware***. Выполняет сканирование приложений в фоновом режиме при их запуске. Подробные сведения >>
- ***Удаленное администрирование***. Подключение экземпляра программы AVG к программе Удаленное администрирование AVG, что позволит сетевому администратору запускать определенные действия приложения удаленно. Компонент Удаленное администрирование будет доступен, только если он был выбран на шаге ***Выбор компонентов*** в ***процессе установки***).
- ***Anti-Rootkit***. Обнаружение программ и средств, пытающихся замаскировать вредоносное ПО. Подробные сведения >>
- ***Лицензия***. Отображение полного текста лицензионного соглашения компании AVG. Подробные сведения >>
- ***Resident Shield***. Работает в фоновом режиме и выполняет сканирование файлов во время их копирования, открытия или сохранения. Подробные сведения >>
- ***Диспетчер обновления***. Предназначен для управления всеми обновлениями AVG. Подробные сведения >>

Щелкните значок компонента один раз, чтобы выделить этот компонент в окне обзора. При этом в нижней части интерфейса пользователя отобразится описание основных функций компонента. Дважды щелкните значок, чтобы открыть интерфейс компонента, содержащий список основных статистических данных.

Откройте контекстное меню, щелкнув значок компонента правой кнопкой мыши. Кроме открытия графического интерфейса компонента, можно также выбрать команду ***Игнорировать состояние компонента***. Выберите эту команду, если известно о состоянии ошибки компонента, но по какой-либо причине не требуется изменять состояние AVG и необходимо отключить оповещение с помощью значка на панели задач.

6.5. Компоненты сервера



Раздел ***Компоненты сервера*** расположен в центральной части интерфейса пользователя AVG. Раздел состоит из двух частей.

- Обзор всех установленных компонентов, состоящих из панели со значком компонента и информации об активности компонента.
- Описание выбранного компонента

В **AVG 9.0 File Server** раздел ***Компоненты сервера*** содержит сведения о следующих компонентах.

- ***Document Scanner для MS SharePoint***. Выполняет сканирование файлов документов, хранящихся в MS SharePoint, и защищает от возможных угроз. Подробнее >>

Щелкните значок компонента один раз, чтобы выделить этот компонент в окне обзора. При этом в нижней части интерфейса пользователя отобразится описание основных функций компонента. Дважды щелкните значок, чтобы открыть интерфейс компонента, содержащий список основных статистических данных.

Откройте контекстное меню, щелкнув правой кнопкой мыши значок компонента. Кроме открытия графического интерфейса компонента, можно также выбрать команду ***Игнорировать состояние компонента***. Выберите эту команду, если известно о состоянии ошибки компонента, но по какой-либо причине не требуется изменять состояние AVG и необходимо отключить оповещение с помощью значка на панели задач.

6.6. Статистика

Раздел ***Статистика*** расположен в левой нижней части интерфейса пользователя AVG. В нем представлены сведения, связанные с работой программы.

- ***Последнее сканирование*** — дата последнего выполненного сканирования.
- ***Последнее обновление*** — дата последнего запуска обновления.
- ***Вирусная БД*** — сведения о версии установленной вирусной базы данных.
- ***Версия AVG*** — сведения о версии установленной программы AVG *(номер отображается в формате 9.0.xx, где 9.0 — это версия серии продуктов, а xx — номер сборки).*
- ***Срок окончания действия лицензии*** — дата окончания срока действия лицензии AVG.

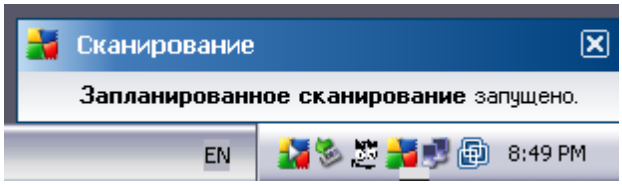
6.7. Значок на панели задач

Значок на панели задач (*на панели задач Windows*) указывает текущее состояние **AVG 9.0 File Server**. Этот значок всегда отображается на панели задач независимо от того, открыто ли главное окно AVG.

Если отображается полным цветом , ***значок на панели задач*** указывает, что все компоненты AVG активны и работают правильно. Кроме того, полноцветный значок AVG на панели задач отображается, если программа AVG находится в состоянии ошибки, но вам известно о проблеме и вы установили параметр ***Игнорировать состояние компонентов***.

Значок с восклицательным знаком указывает на наличие проблемы (*неактивный компонент, состояние ошибки и т. д.*). Дважды щелкните ***значок на панели задач***, чтобы открыть главное окно и настроить необходимый компонент.

Значок на панели задач также может сообщать о выполняемых действиях и возможных изменениях состояния программы AVG (*например, автоматический запуск запланированного сканирования или обновления, изменение состояния компонента, состояние ошибки и т. п.*) с помощью всплывающего окна, открывающегося из значка AVG на панели задач.



Кроме того, дважды щелкнув ***значок на панели задач***, можно быстро получить доступ к главному окну AVG. Если щелкнуть правой кнопкой мыши ***значок на панели задач***, откроется краткое контекстное меню, содержащее следующие пункты.

- ***Открыть интерфейс пользователя AVG***. Открытие интерфейса пользователя AVG
- ***Сканирования***. Открытие контекстного меню предварительно настроенных сеансов сканирования (*Сканирование всего компьютера*, *Сканирование отдельных файлов или папок*, *Сканирование Anti-Rootkit*) и выбор соответствующего варианта. Сканирование будет запущено сразу.
- ***Обновить сейчас***. Немедленный запуск обновления
- ***Справка***. Открытие файла справки на начальной странице.

7. Компоненты AVG

7.1. Anti-Virus

7.1.1. Принципы работы Anti-Virus

Модуль сканирования антивирусного ПО сканирует все файлы и их активность (открытие/закрытие файлов и т. д.) на известные вирусы. Каждый обнаруженный вирус блокируется, удаляется или помещается в карантин. Большая часть антивирусного ПО также использует метод эвристического сканирования, при котором файлы сканируются на типичные признаки вирусов, так называемые "вирусные подписи". Это означает, что антивирусный сканер может обнаружить новый, неизвестный вирус, если новый вирус содержит некоторые типичные признаки уже существующих вирусов.

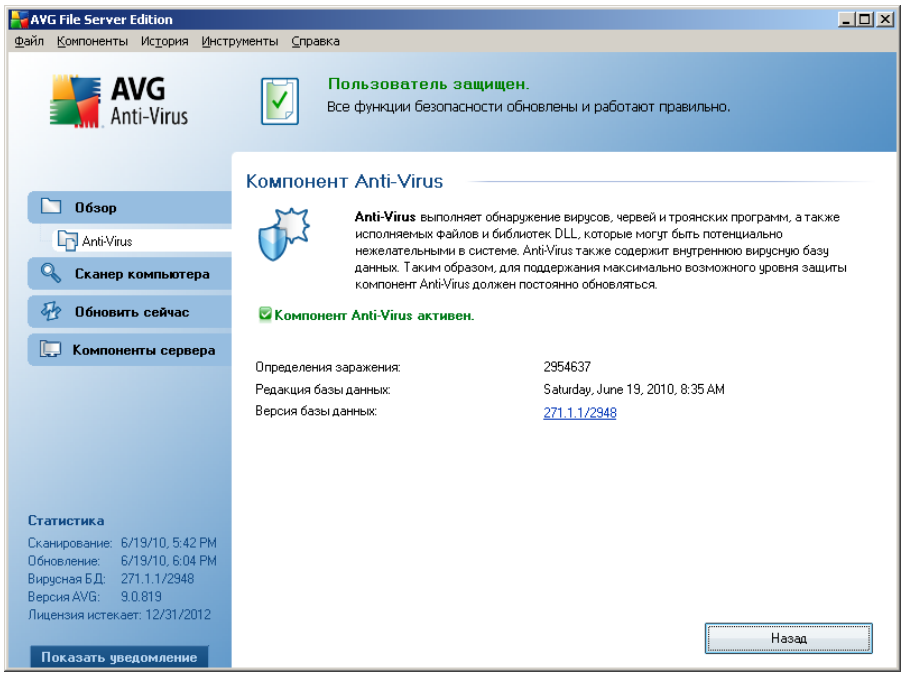
Важной чертой антивирусной защиты является тот факт, что ни один известный вирус не сможет запуститься на компьютере.

Когда одна технология не может справиться с обнаружением и определением вируса, компонент ***Anti-Virus*** использует несколько технологий, чтобы обеспечить защиту компьютера от вирусов.

- Сканирование. Поиск последовательности признаков, характерных для данного вируса.
- Эвристический анализ. Динамическая эмуляция команд сканируемых объектов в виртуальной компьютерной среде.
- Типовое определение. Определение характерных команд данного вируса/ группы вирусов.

Приложение AVG способно анализировать и обнаруживать исполняемые приложения или библиотеки DLL, использование которых в системе может быть потенциально нежелательным. Подобные угрозы называются потенциально нежелательными программами (различные виды шпионского ПО, рекламное ПО и прочее). Более того, AVG сканирует системный реестр на подозрительные записи, временные интернет-файлы, следящие cookie-файлы и позволяет поступать с потенциально вредоносными элементами так же, как и с другими зараженным объектами.

7.1.2. Интерфейс Anti-Virus



Интерфейс компонента ***Anti-Virus*** предоставляет краткий обзор функциональности компонента, сведения о текущем состоянии компонента (*Компонент Anti-Virus активен.*), а также краткий обзор статистики компонента ***Anti-Virus***.

- ***Определения заражений*** — количество вирусов, определенных в последней версии вирусной базы данных
- ***Последнее обновление базы данных*** — дата и время последнего обновления базы данных
- ***Версия базы данных*** — номер последней версии вирусной базы данных; в результате каждого обновления вирусной базы данных номер увеличивается

Для интерфейса данного компонента доступна только одна кнопка управления (***Назад***). Нажмите эту кнопку, чтобы вернуться к интерфейсу пользователя AVG, установленному по умолчанию (обзор компонентов).

Примечание. *Все компоненты AVG настроены поставщиком ПО для обеспечения оптимального качества работы. Не изменяйте настройки AVG без необходимости.*

*Все изменения настроек должны выполняться опытным пользователем. При необходимости изменить настройки AVG выберите элемент системного меню **Инструменты/Дополнительные настройки** и исправьте настройки AVG во вновь открытом диалоговом окне Расширенные настройки AVG.*

7.2. Anti-Spyware

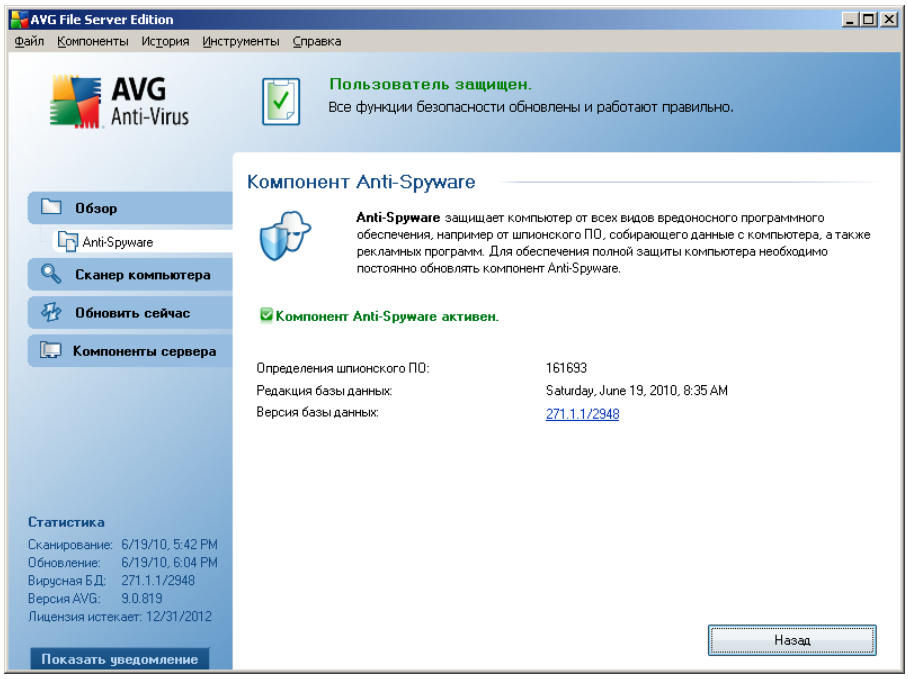
7.2.1. Принципы работы Anti-Spyware

Шпионское программное обеспечение — это тип вредоносного ПО, собирающего информацию на компьютерах пользователей без их ведома или согласия. Некоторые шпионские приложения устанавливаются осознанно и часто содержат рекламу, всплывающие окна или различные типы нежелательного ПО.

В настоящее время основным источником заражений являются веб-сайты с потенциально опасным содержимым. Кроме того, шпионское ПО может распространяться по электронной почте, а также в виде червей или вирусов. Самым эффективным средством защиты от перечисленных угроз является использование сканера ***Anti-Spyware***, работающего постоянно в фоновом режиме, аналогичного компоненту Resident Shield, который сканирует приложения при их запуске.

Также существует потенциальная опасность того, что вредоносное ПО может попасть на компьютер до установки программы AVG, а также если пользователь пренебрег обновлением базы данных **AVG 9.0 File Server** и загрузкой обновлений программы. В таких случаях программа AVG предложит выполнить полное сканирование компьютера на наличие вредоносного или шпионского ПО с помощью функции сканирования. При сканировании также можно обнаружить "спящее" и неактивное вредоносное ПО, то есть вредоносное ПО, которое загружено, но еще не активировано.

7.2.2. Интерфейс Anti-Spyware



Интерфейс компонента ***Anti-Spyware*** содержит краткий обзор функций компонента, сведения о текущем состоянии компонента (компонент *Anti-Spyware активен.*), а также некоторые сведения статистики ***Anti-Spyware***:

- ***Определение шпионского ПО***. Обеспечивает подсчет образцов шпионского ПО, определенного в последней версии базы данных шпионского ПО.
- ***Последнее обновление базы данных*** — определяет, когда и в какое время была обновлена база данных шпионского ПО
- ***Версия базы данных*** — определяет номер последней версии вирусной базы данных; в результате каждого обновления вирусной базы данных номер увеличивается

Для интерфейса данного компонента доступна только одна кнопка управления (***Назад***). Нажмите эту кнопку, чтобы вернуться к интерфейсу пользователя AVG, установленному по умолчанию (обзор компонентов).

Примечание. *Все компоненты AVG настроены поставщиком ПО для обеспечения оптимального качества работы. Не изменяйте настройки AVG без необходимости.*

*Все изменения настроек должны выполняться опытным пользователем. При необходимости изменить настройки AVG выберите элемент системного меню **Инструменты/Дополнительные настройки** и исправьте настройки AVG во вновь открытом диалоговом окне Расширенные настройки AVG.*

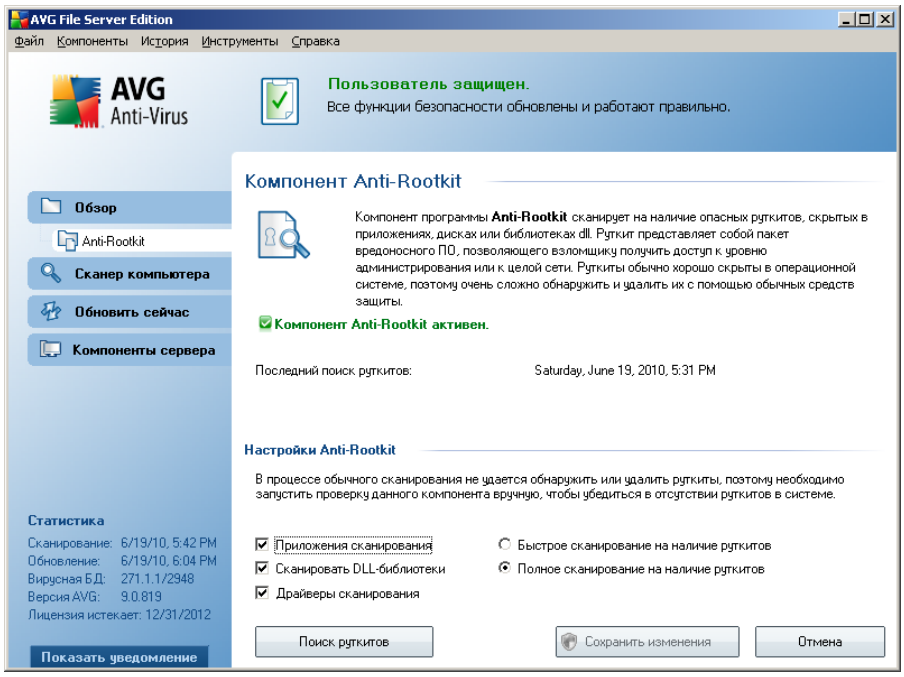
7.3. Anti-Rootkit

Rootkit — это программа, предназначенная для полного управление системой компьютера без разрешения владельцев систем или законных управляющих. Средствам rootkit обычно не требуется доступ к оборудованию, так как они предназначены для управления операционными системами, установленными на этом оборудовании. В большинстве случаев средства rootkit скрывают свое присутствие в системе с помощью замены информации или обхода стандартных механизмов безопасности операционных систем. Кроме того, они могут попадать на компьютер в виде троянских программ, которые пользователи уверенно запускают, не подозревая об опасности. Используемые для этого технические приемы включают в себя скрытие запущенных процессов от следящих программ, а файлов и системных данных — от операционных систем.

7.3.1. Принципы работы Anti-Rootkit

AVG Anti-Rootkit — это специализированный инструмент, предназначенный для обнаружения и эффективного удаления опасных средств rootkit, то есть программ и технологий, позволяющих скрывать вредоносное ПО, присутствующее на компьютере. Компонент ***AVG Anti-Rootkit*** позволяет обнаруживать средства rootkit с помощью предварительного настроенного набора правил. Имейте ввиду, что обнаруживаются все средства rootkit (*не только зараженные*). Если компонент ***AVG Anti-Rootkit*** обнаружил средство rootkit, это еще не значит, что обнаруженный объект заражен. Иногда средства rootkit используются в качестве драйверов или являются частью приложений.

7.3.2. Интерфейс Anti-Rootkit



В интерфейсе пользователя ***Anti-Rootkit*** приводится краткое описание функций компонента, а также сведения о текущем состоянии компонента (*Компонент Anti-Rootkit активен.*) и последнем запуске проверки с помощью компонента ***Anti-Rootkit***.

В нижней части диалогового окна расположен раздел ***Параметры Anti-Rootkit***, в котором можно настроить некоторые из основных функций сканирования на наличие средств rootkit. Чтобы указать объекты, которые должны сканироваться, установите соответствующие флажки.

- ***Сканировать приложения***
- ***Сканировать DLL-библиотеки***
- ***Сканировать драйверы***

Далее можно включить режим сканирования на наличие средств rootkit.

- ***Быстрое сканирование rootkit*** — сканирование только системной папки (*обычно c:\Windows*)

- ***Полное сканирование rootkit*** — сканирование всех доступных дисков, за исключением дисков A: и B:.

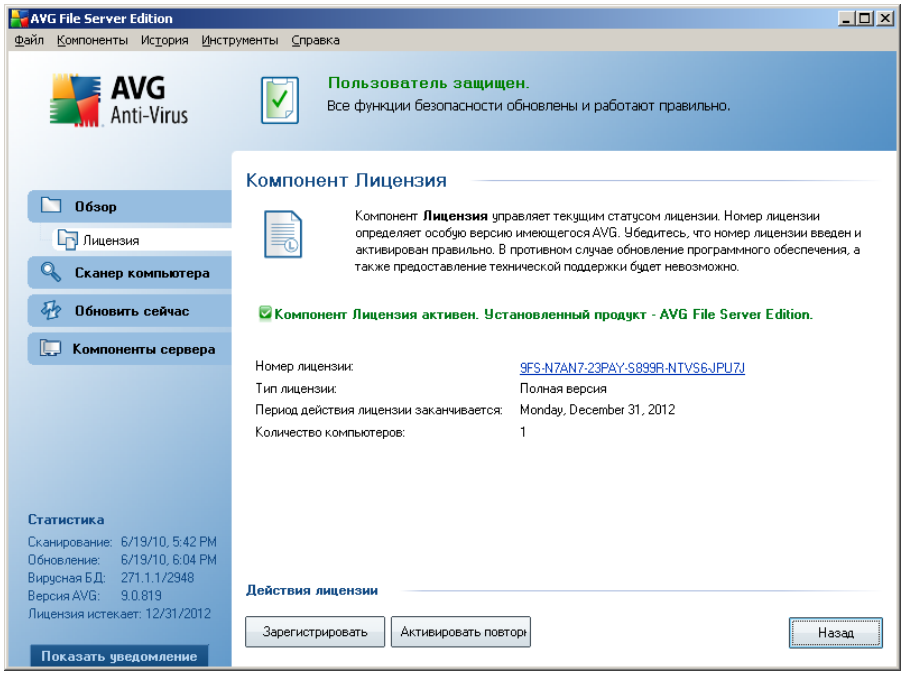
Доступные кнопки управления.

- ***Поиск средств rootkits*** — так как сканирование на наличие средств rootkit не выполняется при выборе типа сканирования ***Сканирование всего компьютера***, его можно запустить непосредственно в интерфейсе ***Anti-Rootkit*** с помощью данной кнопки

- ***Сохранить изменения*** — нажмите данную кнопку, чтобы сохранить все изменения, произведенные в данном интерфейсе, и вернуться к ***интерфейсу пользователя AVG*** по умолчанию (обзор компонентов)

- ***Отмена*** — используйте данную кнопку для возврата к ***интерфейсу пользователя AVG*** по умолчанию (обзор компонентов) без сохранения изменений

7.4. Лицензия



С помощью интерфейса компонента ***Лицензия*** можно получить краткие сведения о работе компонента и информацию о текущем состоянии (*компонент "Лицензия"*

активен.), а также следующую информацию.

- ***Номер лицензии***. Номер лицензии продукта. Необходимо правильно ввести номер лицензии. Настоятельно рекомендуется использовать способ "копировать/вставить" для любых операций с номером лицензии.

- ***Тип лицензии***. Тип устанавливаемого продукта.

- ***Срок окончания действия лицензии***. Данная дата определяет период действия лицензии. Чтобы использовать **AVG 9.0 File Server** после окончания срока действия лицензии, потребуется выполнить продление срока действия лицензии. Обновление лицензии может быть выполнено в Интернете на веб-сайте AVG (http://www.avg.com).

- ***Количество компьютеров***. Количество рабочих станций, на которые пользователь может установить приложение **AVG 9.0 File Server**.

Кнопки управления

- ***Регистрация***. Переход на страницу регистрации веб-сайта комании AVG (http://www.avg.com). Введите данные для регистрации. Только клиенты, зарегистрировавшие продукт AVG, могут получать бесплатную техническую поддержку.

- ***Активировать повторно***. Открытие диалогового окна ***Активация AVG***, содержащего сведения, введенные в диалоговое окно ***Персонализация AVG*** при установке. В данном диалоговом окне можно ввести номер лицензии, чтобы заменить им номер продажи (*номер, который использовался при установке AVG*) или заменить старый номер лицензии (*например, при обновлении до нового продукта AVG*).

- ***Назад*** . Нажмите данную кнопку для возврата к установленному по умолчанию интерфейсу пользователя AVG (обзор компонентов).

7.5. Resident Shield

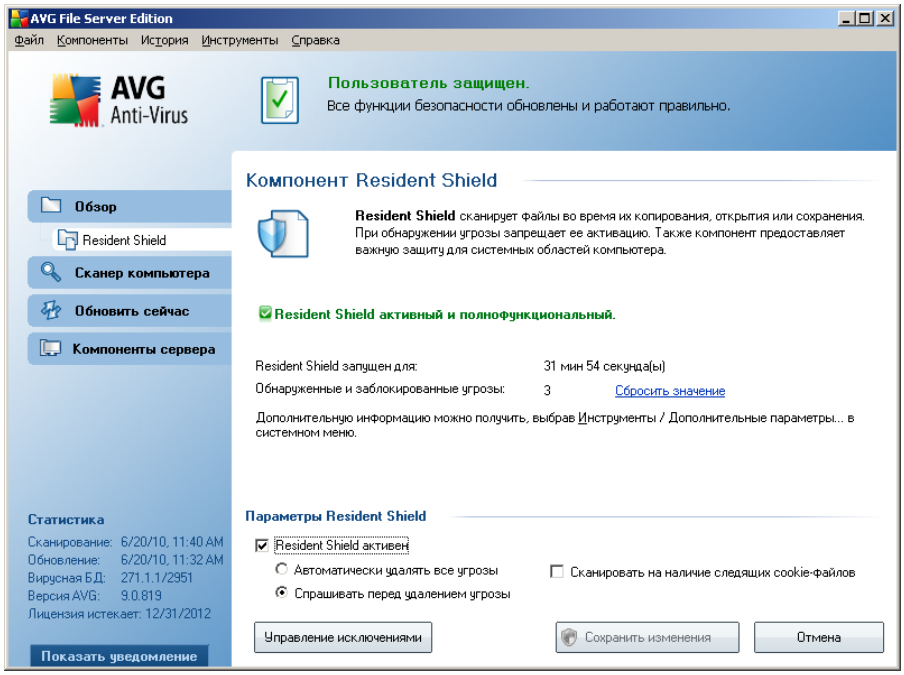
7.5.1. Принципы работы Resident Shield

Компонент ***Resident Shield*** обеспечивает непрерывную защиту компьютера. Он сканирует каждый файл при открытии, сохранении или копировании и защищает системные области компьютера. Если при доступе к файлу компонент ***Resident Shield*** обнаруживает вирус, все выполняемые в данный момент действия с файлом

завершаются. Таким образом, вирус не может активировать себя. Обычно процесс сканирования незаметен, так как протекает в фоновом режиме, а уведомления отображаются только при обнаружении угроз. Однако компонент ***Resident Shield*** блокирует активацию угрозы и удаляет ее. Компонент ***Resident Shield*** загружается в память компьютера при запуске системы.

Предупреждение. Компонент Resident Shield загружается в память компьютера при запуске системы — крайне необходимо, чтобы данный компонент всегда был запущен.

7.5.2. Интерфейс Resident Shield



Помимо обзора наиболее важных статистических сведений и информации о

текущем состоянии компонента (*Компонент Resident Shield активен и работает правильно*), интерфейс компонента ***Resident Shield*** также позволяет настроить некоторые основные параметры. В интерфейсе компонента отображается следующая статистическая информация.

- ***Время работы компонента Resident Shield***. Время, прошедшее с момента запуска компонента.
- ***Обнаруженные и заблокированные угрозы***. Количество обнаруженных заражений, запуск/открытие которых удалось предотвратить (*при необходимости данное значение можно сбросить; например, в статистических целях — Сбросить значение*).

Базовая настройка компонента

В нижней части диалогового окна расположен раздел ***Параметры Resident Shield*** , который позволяет изменять некоторые основные параметры компонента (*подробные настройки, как и в других компонентах, доступны в системном меню Инструменты/Дополнительные параметры*).

Параметр ***Компонент Resident Shield активен*** позволяет легко включать и отключать постоянную защиту. По умолчанию данная функция включена. Если постоянная защита включена, можно определить действия, которые будут производиться с обнаруженными заражениями (удалено):

- автоматически (***Удалять все угрозы автоматически***);
- или только после подтверждения пользователем (***Запрашивать подтверждение перед удалением угроз***).

Данный параметр не влияет на уровень безопасности, поэтому может быть настроен на усмотрение пользователя.

В обоих случаях можно также выбрать параметр ***Удалять файлы cookie автоматически.*** В некоторых случаях может потребоваться включение данного параметра, чтобы обеспечить максимальный уровень безопасности. Однако по умолчанию параметр отключен. (*cookies = текстовые пакеты, отправляемые сервером в веб-браузер, а затем веб-браузером обратно на сервер при каждом подключении браузера к серверу. Файлы cookie протокола HTTP используются для проверки подлинности, отслеживания и сбора определенной информации о пользователях, например о предпочитаемых сайтах или содержимом корзин для покупок в Интернете*).

Примечание. *Все компоненты AVG настроены поставщиком ПО для обеспечения оптимального качества работы. Не изменяйте настройки AVG без необходимости. Все изменения настроек должны выполняться опытным пользователем. При необходимости изменить настройки AVG выберите элемент системного меню* ***Инструменты/Дополнительные настройки*** *и исправьте настройки AVG во вновь открытом диалоговом окне Расширенные настройки AVG.*

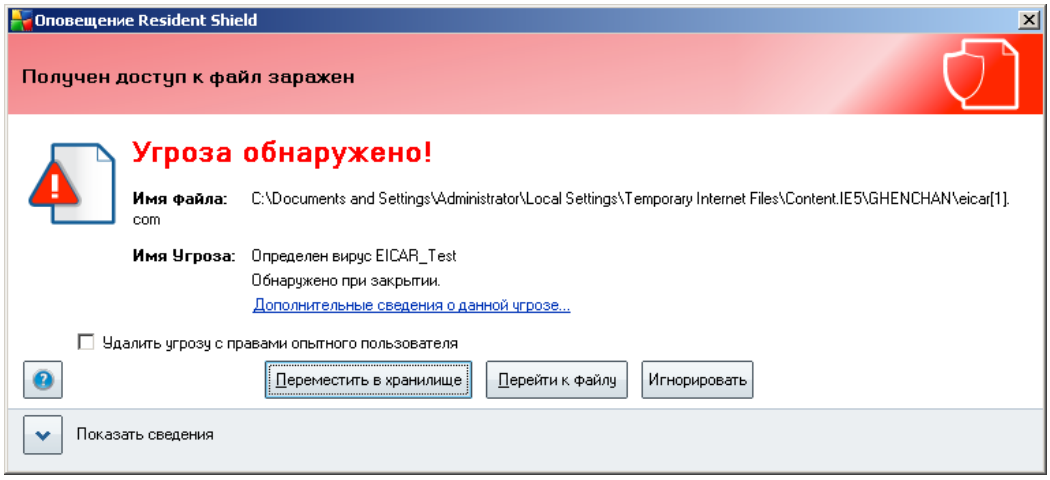
Кнопки управления

В интерфейсе компонента ***Resident Shield*** доступны следующие кнопки управления.

- ***Управление исключениями***. Открытие нового диалогового окна, в котором можно определить папки и файлы, которые не требуется сканировать с помощью ***Resident Shield*** (дополнительные сведения об этом диалоговом окне см. в разделах ***Исключаемые каталоги*** и ***Исключаемые файлы***).
- ***Сохранить изменения***. Нажмите данную кнопку для сохранения и применения изменений, выполненных в данном диалоговом окне
- ***Отмена***. Нажмите данную кнопку для возврата к установленному по умолчанию ***интерфейсу пользователя AVG*** (обзор компонентов)

7.5.3. Обнаружение Resident Shield

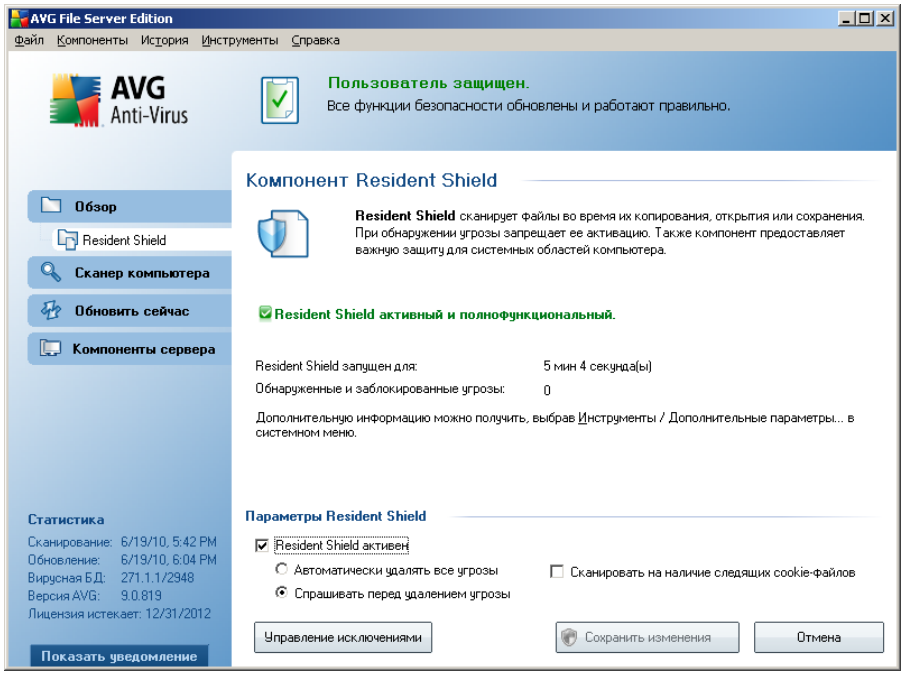
Resident Shield сканирует копируемые, открываемые или сохраняемые файлы. При обнаружении вируса или угрозы сразу же появляется предупреждение в следующем диалоговом окне.



Диалоговое окно предоставляет информацию об обнаруженной угрозе и предлагает возможные действия.

- ***Вылечить***. Если лечение возможно, AVG вылечит зараженный файл автоматически, рекомендуется именно это действие.
- ***Поместить в хранилище***. Вирус будет помещен в ***хранилище вирусов AVG***
- ***Перейти к файлу***. Перенаправление в папку размещения подозрительного объекта (*в новом окне Проводника Windows*).
- ***Игнорировать***. Категорически не рекомендуется использовать данный параметр.

Полный обзор всех угроз, обнаруженных компонентом ***Resident Shield***, доступен в окне ***Обнаружение Resident Shield*** в системном меню ***История/Обнаружения Resident Shield***.



В диалоговом окне ***Обнаружение Resident Shield*** представлен обзор объектов, обнаруженных компонентом ***Resident Shield*** и определенных как опасные, которые были вылечены или помещенные в ***Хранилище вирусов***. Для каждого обнаруженного объекта предоставляется следующая информация.

- ***Заражение***. Описание (возможно, даже имя) обнаруженного объекта.
- ***Объект***. Местоположение объекта.
- ***Результат***. Действие, выполненное в отношении обнаруженного объекта.
- ***Время обнаружения***. Дата и время обнаружения объекта.
- ***Тип объекта***. Тип обнаруженного объекта.
- ***Процесс***. Действия, предпринятые для обнаружения потенциально опасного объекта.

В нижней части диалогового окна под списком находится информация об общем количестве обнаруженных объектов, перечисленных выше. Также можно экспортировать весь список обнаруженных объектов в файл (***Экспортировать список в файл***) и удалить все записи об обнаруженных объектах (***Очистить список***). Кнопка ***Обновить список*** обновит список объектов, найденных

компонентом ***Resident Shield***. С помощью кнопок ***Удалить выбранные угрозы*** и ***Удалить все угрозы*** можно переместить выбранные (или все показанные) угрозы в хранилище вирусов. Кнопка ***Назад*** выполняет переключение к ***интерфейсу пользователя AVG*** (по умолчанию обзор компонентов).

7.6. Диспетчер обновления

7.6.1. Принципы работы диспетчера обновления

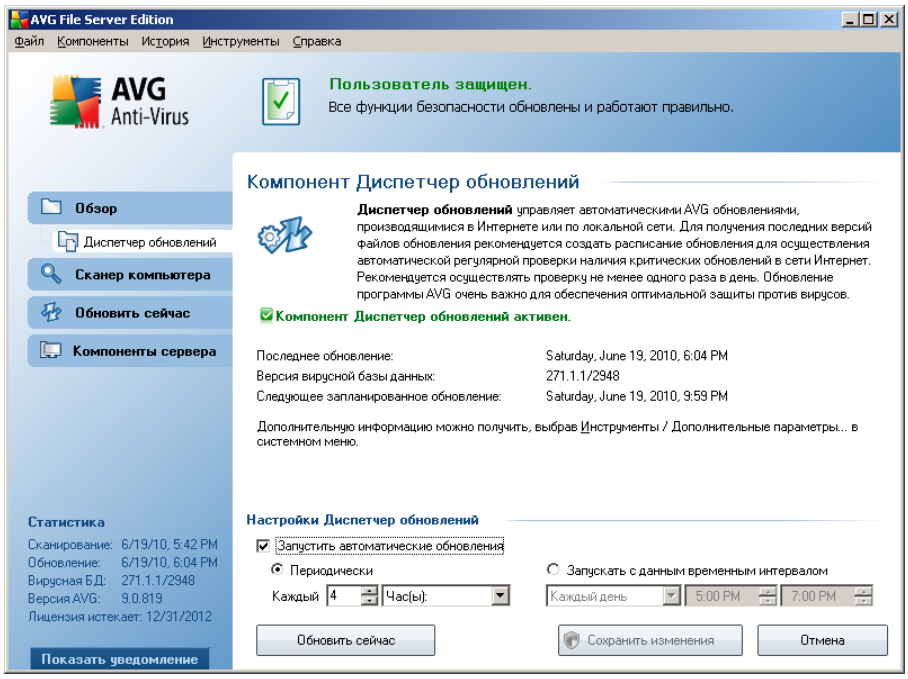
Ни один из программных продуктов по обеспечению безопасности не может гарантировать полноценную защиту от различных типов угроз без регулярного обновления. Создатели вирусов ищут новые уязвимые места для взлома программного обеспечения и операционных систем. Ежедневно совершаются попытки несанкционированного доступа, появляются новые вирусы и вредоносное ПО. Именно поэтому поставщиками программного обеспечения постоянно выпускаются обновления и исправления для систем безопасности, предназначенные для исправления обнаруженных уязвимостей.

Очень важно выполнять регулярное обновление продуктов AVG!

Управлять регулярными обновлениями можно с помощью компонента ***Диспетчер обновления***. Данный компонент позволяет запланировать автоматическую загрузку файлов обновлений через Интернет или локальную сеть. Важные обновления определений вирусов должны выполняться ежедневно, если это возможно. Обновление менее важных программ может выполняться один раз в неделю.

Примечание. *Для получения дополнительной информации о типах и уровнях обновлений внимательно ознакомьтесь с разделом Обновления AVG.*

7.6.2. Интерфейс диспетчера обновления



В интерфейсе компонента ***Диспетчер обновления*** можно просмотреть сведения о функциях и текущем состоянии компонента (*Диспетчер обновления активен.*), а также важные статистические данные.

- ***Последнее обновление*** — дата и время последнего обновления базы данных
- ***Версия вирусной базы данных*** — номер последней версии вирусной базы данных; в результате каждого обновления вирусной базы данных номер увеличивается
- ***Следующее запланированное обновление*** — дата и время следующего запланированного обновления базы данных

Основные настройки компонента

В·нижней·части·диалогового·окна·расположен·раздел·***Параметры·компонента·"Диспетчер обновления"***, где можно изменить правила запуска процесса обновления. Файлы обновления могут загружаться автоматически (***Запустить автоматические обновления***) или по требованию.

Функция ***Запустить автоматические обновления*** включена по умолчанию. Данную настройку изменять не рекомендуется. Регулярная загрузка файлов обновлений имеет решающее значение для правильной работы ПО по обеспечению безопасности.

Также можно определить время запуска процесса обновления.

- ***Периодически*** — позволяет определить временной интервал
- ***В указанное время*** — позволяет задать точные дату и время

По умолчанию обновление выполняется каждые 4 часа. Рекомендуется изменять данную настройку только в случае крайней необходимости.

Примечание. *Все компоненты AVG настроены поставщиком ПО для обеспечения оптимального качества работы. Не изменяйте настройки AVG без необходимости. Все изменения настроек должны выполняться опытным пользователем. При необходимости изменить настройки AVG выберите элемент системного меню* ***Инструменты/Дополнительные настройки*** *и исправьте настройки AVG во вновь открытом диалоговом окне Расширенные настройки AVG.*

Кнопки управления

В интерфейсе компонента ***Диспетчер обновления*** имеются следующие кнопки управления.

- ***Обновить сейчас*** — запускает немедленное обновление по требованию
- ***Сохранить изменения*** — нажмите данную кнопку для сохранения и применения изменений, выполненных в данном диалоговом окне
- ***Отмена***. Нажмите данную кнопку для возврата к установленному по умолчанию ***интерфейсу пользователя AVG*** (обзор компонентов)

8. Компоненты сервера AVG

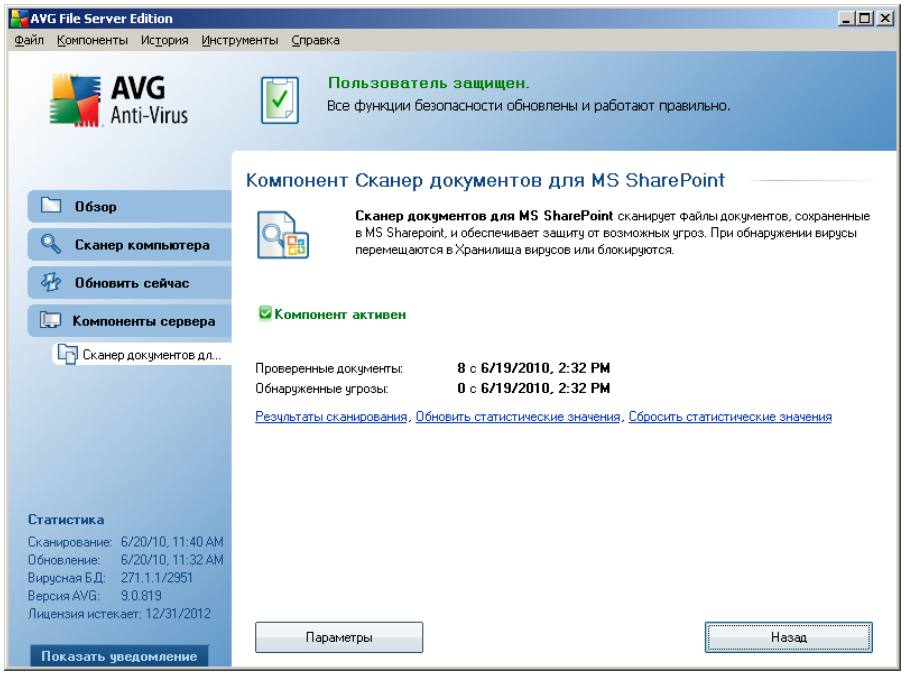
8.1. Documents Scanner для MS SharePoint

8.1.1. Принципы работы Document Scanner

Серверный компонент ***Document Scanner для MS SharePoint*** выполняет сканирование документов, хранящихся в MS SharePoint. При обнаружении вирусов документы перемещаются в хранилище вирусов или полностью удаляются.

Microsoft SharePoint — это набор продуктов и программных элементов, который включает в себя (кроме постоянно растущего набора компонентов) функции совместной работы на основе обозревателя Internet Explorer, модули управления процессами, поисковые модули и платформу управления документами. SharePoint можно использовать для размещения веб-сайтов, предоставляющих доступ к общим рабочим областям, банкам данных и документам.

8.1.2. Интерфейс Document Scanner



Наряду с обзором наиболее важных статистических данных и сведений о текущем

состоянии компонента (*Компонент активен*) интерфейс ***Documents Scanner для MS SharePoint*** предоставляет краткие сведения о статистике компонента.

- ***Проверенные документы***. Количество документов, проверенных с определенной даты.
- ***Обнаруженные угрозы***. Количество угроз, обнаруженных с определенной даты.

Эту статистику можно обновить в любое время, щелкнув ссылку ***Обновить статистические значения***. Новые данные отобразятся практически сразу. Чтобы обнулить все статистические значения, щелкните ссылку ***Сбросить статистические значения***. Наконец, если щелкнуть ссылку ***Результаты сканирования***, откроется новое диалоговое окно со списком результатов сканирования. Отсортируйте данные в списке, используя переключатели и/или вкладки.

Кнопки управления

В интерфейсе компонента ***Documents Scanner для MS SharePoint*** имеются следующие кнопки управления.

- ***Параметры***. Открытие нового диалогового окна, в котором можно настроить некоторые параметры, связанные с производительностью сканирования документов на наличие вирусов компонентом ***Document Scanner для MS SharePoint*** (дополнительную информацию об этом диалоговом окне см. в разделах ***Дополнительные параметры Document Scanner для MS SharePoint*** и ***Действия по обнаружению***).
- ***Назад***. Нажмите эту кнопку, чтобы вернуться к интерфейсу по умолчанию ***Компоненты сервера***.

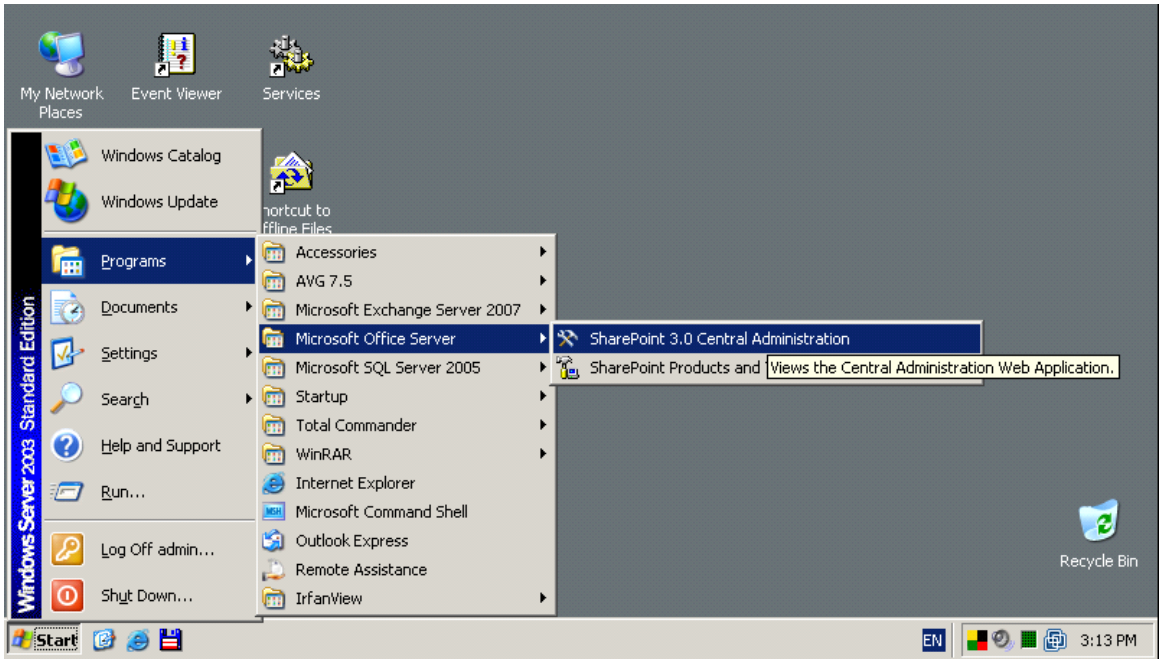
9. AVG для SharePoint Portal Server

Данный раздел посвящен обслуживанию программы AVG на сервере ***MS SharePoint Portal Server***, который является особой разновидностью файловых серверов.

9.1. Обслуживание программы

AVG для SharePoint Portal Server использует интерфейс сканирования вирусов Microsoft SP VSAPI 1.4 для защиты сервера от возможных заражений вирусами. Объекты на сервере проверяются на наличие вредоносного ПО при загрузке или выгрузке с сервера пользователями. Конфигурацию защиты от вирусов можно настроить с помощью интерфейса ***Центр администрирования*** сервера SharePoint Portal Server. В модуле ***Центр администрирования*** также можно просматривать и управлять файлом журнала **AVG для SharePoint Portal Server**.

Компонент ***Центр администрирования SharePoint Portal Server*** можно запустить после входа в систему компьютера, на котором установлен сервер. Компонент администрирования имеет веб-интерфейс (*аналогичный пользовательскому интерфейсу сервера SharePoint Portal Server*). Для доступа к нему выберите ***Центр администрирования SharePoint (3.0)*** в папке ***Программы/Microsoft Office Server*** (***или SharePoint Portal Server***) в меню ***Пуск*** операционной системы Windows.

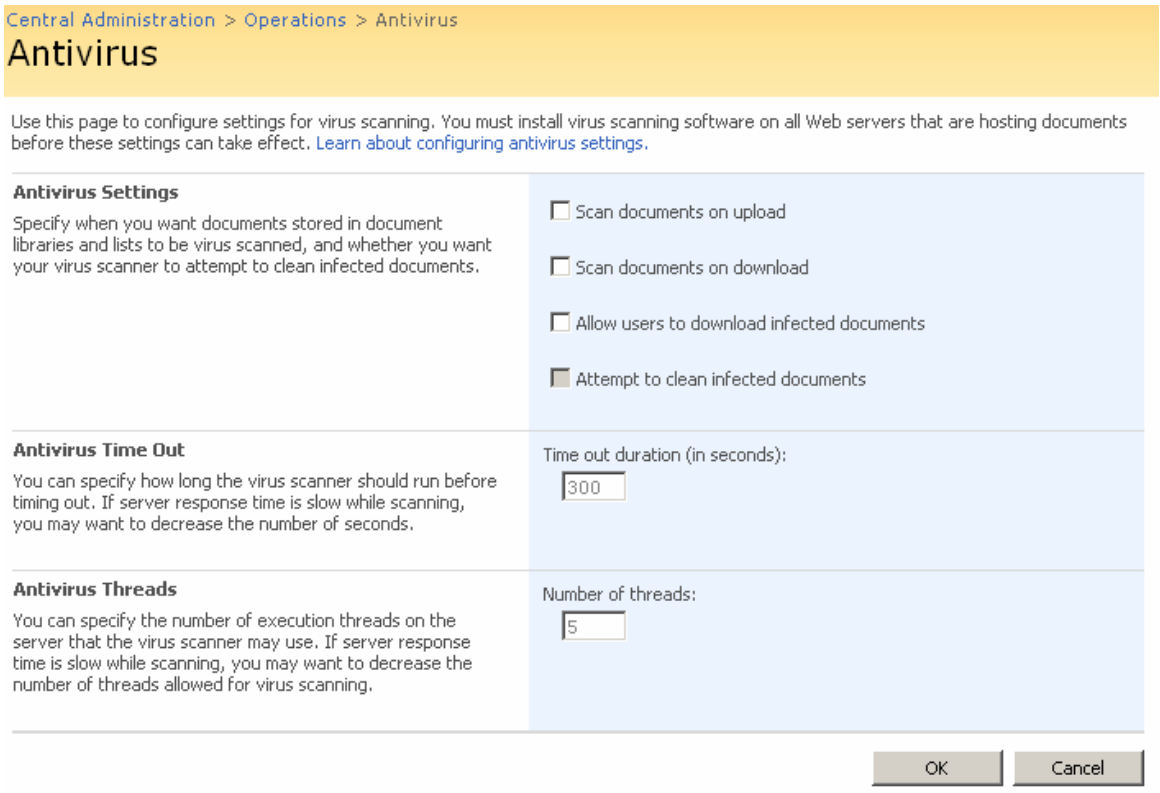


На веб-страницу ***Центр администрирования SharePoint Portal Server*** также можно перейти удаленно при наличии необходимых прав доступа и правильного URL-адреса.

9.2. Конфигурация AVG для SPPS — SharePoint 2007

В интерфейсе ***Центр администрирования SharePoint 3.0*** можно с легкостью настроить параметры производительности и действия сканера **AVG для SharePoint Portal Server**. Выберите параметр ***Операции*** в разделе ***Центр администрирования***. Откроется новое диалоговое окно. Выберите ***Anti-Virus*** в разделе ***Конфигурация защиты***.

Откроется следующее окно.



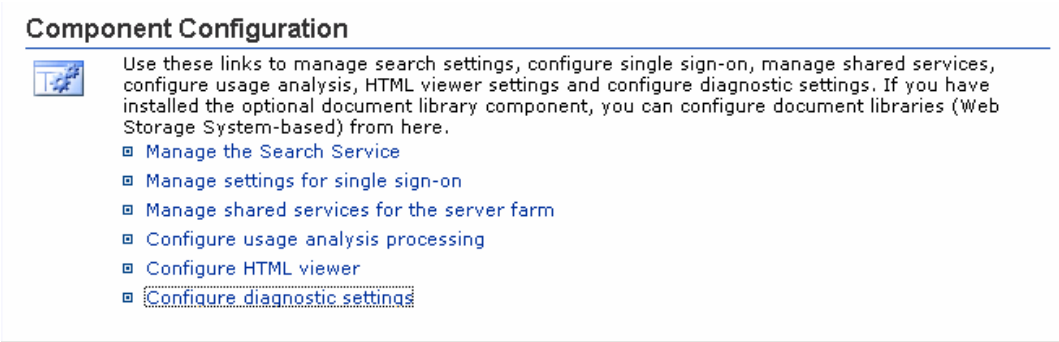
В нем можно настроить различные параметры производительности и сканирования компонента Anti-Virus **AVG для SharePoint Portal Server**.

- ***Сканировать документы при загрузке с компьютера***. Включение/выключение сканирования документов, загружаемых с компьютера
- ***Сканировать документы при загрузке на компьютер***. Включение/выключение сканирования документов, загружаемых на компьютер
- ***Разрешать пользователям загружать зараженные документы***. Разрешение/запрет на загрузку пользователями зараженных документов
- ***Попытаться очистить зараженный документ***. Включение/отключение функции автоматической очистки зараженных документов
- ***Временное ограничение*** (*в секундах*). Максимальное количество секунд, в течение которого будет выполняться сканирование на вирусы после запуска (уменьшите значение, если при сканировании документов увеличилось время отклика сервера)

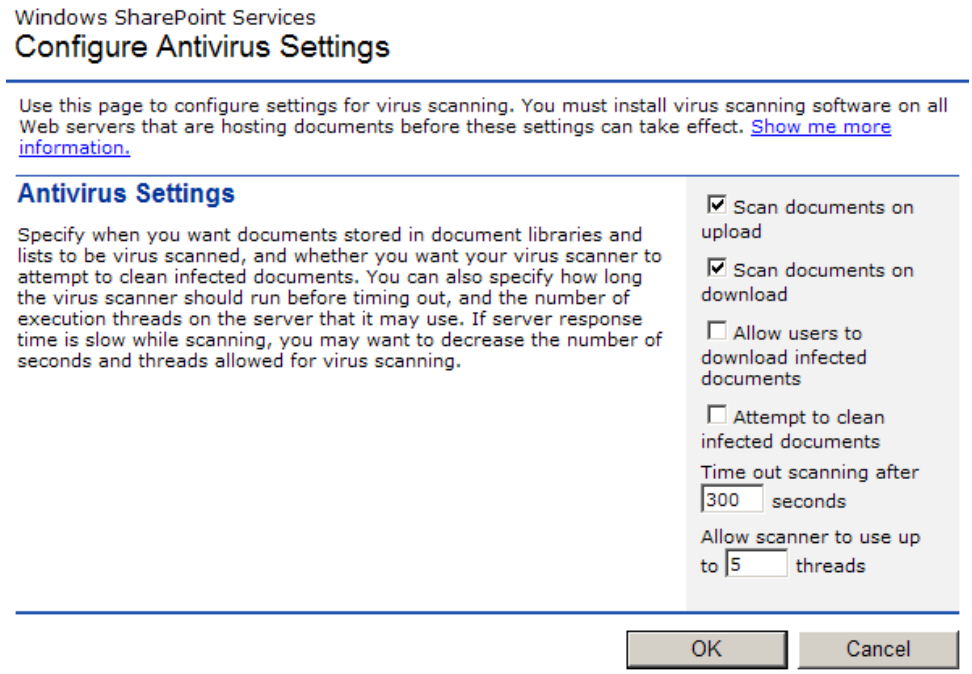
- ***Количество одновременных процессов***. Определение количества операций сканирования на вирусы, которые могут быть запущены одновременно; увеличив данное значение, можно ускорить процесс сканирования за счет его параллельного выполнения, однако это также может привести к увеличению времени отклика сервера.

9.3. Конфигурация AVG для SPPS — SharePoint 2003

В интерфейсе ***Центр администрирования SharePoint Portal Server*** можно с легкостью настроить параметры производительности и действия сканера **AVG для SharePoint Portal Server**. Выберите параметр ***Конфигурация действий антивирусного ПО*** в разделе ***Конфигурация защиты***.



Откроется следующее окно.



В нем можно настроить различные параметры производительности и сканирования компонента Anti-Virus **AVG для SharePoint Portal Server**.

- ***Сканировать документы при загрузке с компьютера***. Включение/выключение сканирования документов, загружаемых с компьютера
- ***Сканировать документы при загрузке на компьютер***. Включение/выключение сканирования документов, загружаемых на компьютер
- ***Разрешать пользователям загружать зараженные документы***. Разрешение/запрет на загрузку пользователями зараженных документов
- ***Попытаться очистить зараженный документ***. Включение/отключение функции автоматической очистки зараженных документов
- ***Временное ограничение сканирования***. Максимальное количество секунд, в течение которого будет выполняться сканирование на вирусы после запуска (*уменьшите значение, если при сканировании документов увеличилось время отклика сервера*)
- ***Использовать макс. X подпроцессов при сканировании документов***. "X" определяет количество операций сканирования на вирусы, которые

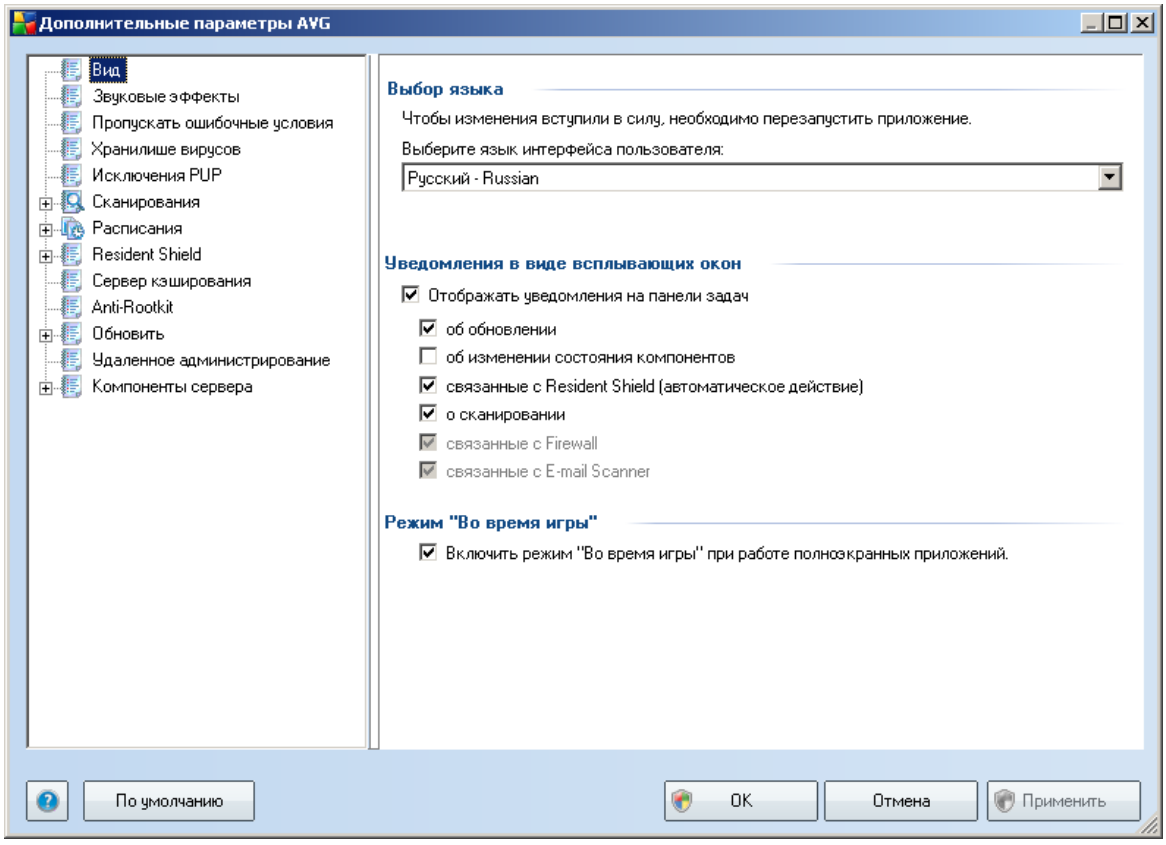
могут быть запущены одновременно; увеличив данное значение, можно ускорить процесс сканирования за счет его параллельного выполнения, однако это также может привести к увеличению времени отклика сервера.

10. Расширенные параметры AVG

Параметры дополнительной настройки **AVG 9.0 File Server** откроются в новом диалоговом окне ***Дополнительные параметры AVG***. Окно разделено на две части. В левой части расположено навигационное дерево параметров программы. Выберите компонент, параметры которого необходимо изменить (*или часть компонента*), чтобы открыть диалоговое окно редактирования в правой части окна.

10.1. Внешний вид

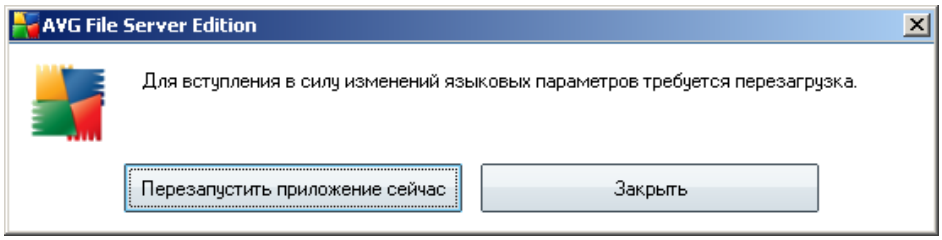
Параметр ***Вид***, первый элемент навигационного дерева, относится к общим параметрам интерфейса пользователя AVG и нескольким начальным параметрам поведения приложения.



Выбор языка

В раскрывающемся меню раздела ***Выбор языка*** можно выбрать необходимый язык; после этого интерфейс пользователя AVG будет отображаться на выбранном языке. В раскрывающемся меню отображаются только языки, выбранные ранее в процессе установки программы (см. раздел Выборочная установка — выбор компонентов). Чтобы завершить процесс смены языка приложения, необходимо перезапустить интерфейс пользователя; выполните следующие действия.

- Выберите необходимый язык приложения и подтвердите выбор, нажав кнопку ***Применить*** (в правом нижнем углу).
- Для подтверждения нажмите кнопку ***OK***
- Новые всплывающие диалоговые окна информируют о том, что для повторного запуска приложения требуется смена языка интерфейса пользователя AVG:



Уведомления в виде всплывающих окон на панели задач

В данном разделе можно отключить отображение уведомлений о состоянии приложения в виде всплывающих окон на панели задач. По умолчанию отображение уведомлений в виде всплывающих окон включено. Рекомендуется не отключать данный параметр. Уведомления в виде всплывающих окон обычно информируют пользователя об изменениях состояния какого-либо компонента AVG. Необходимо обращать на них внимание.

Однако, если по какой-либо причине необходимо отключить данные уведомления или настроить отображение только определенных уведомлений (связанных с каким-либо компонентом AVG), то это можно сделать, установив или сняв флажки с соответствующих параметров.

- ***Отображать уведомления на панели задач***. По умолчанию данный параметр отмечен флажком (*включен*), а уведомления отображаются. Снимите флажок с данного параметра, чтобы отключить отображение всех всплывающих уведомлений. Если данный параметр включен, можно настроить отображение отдельных уведомлений.

- ***Отображать уведомления об обновлении*** на панели задач. Позволяет определить, следует ли отображать информацию о запуске процесса обновления AVG, его состоянии и завершении.

- ***Отображать уведомления об изменении состояния компонентов*** . Позволяет определить, должна ли отображаться информация об активности/бездействии компонента или о его возможных проблемах. При сообщении о состоянии ошибки компонента данный параметр работает аналогично информативной функции значка на панели задач (изменение цвета), сообщая о проблеме компонента AVG *(данный параметр является единственным отключенным по умолчанию)*.

- ***Отображать уведомления о Resident Shield на панели задач***. Определяет, будут ли отображаться сведения о сохранении, копировании и открытии файлов.

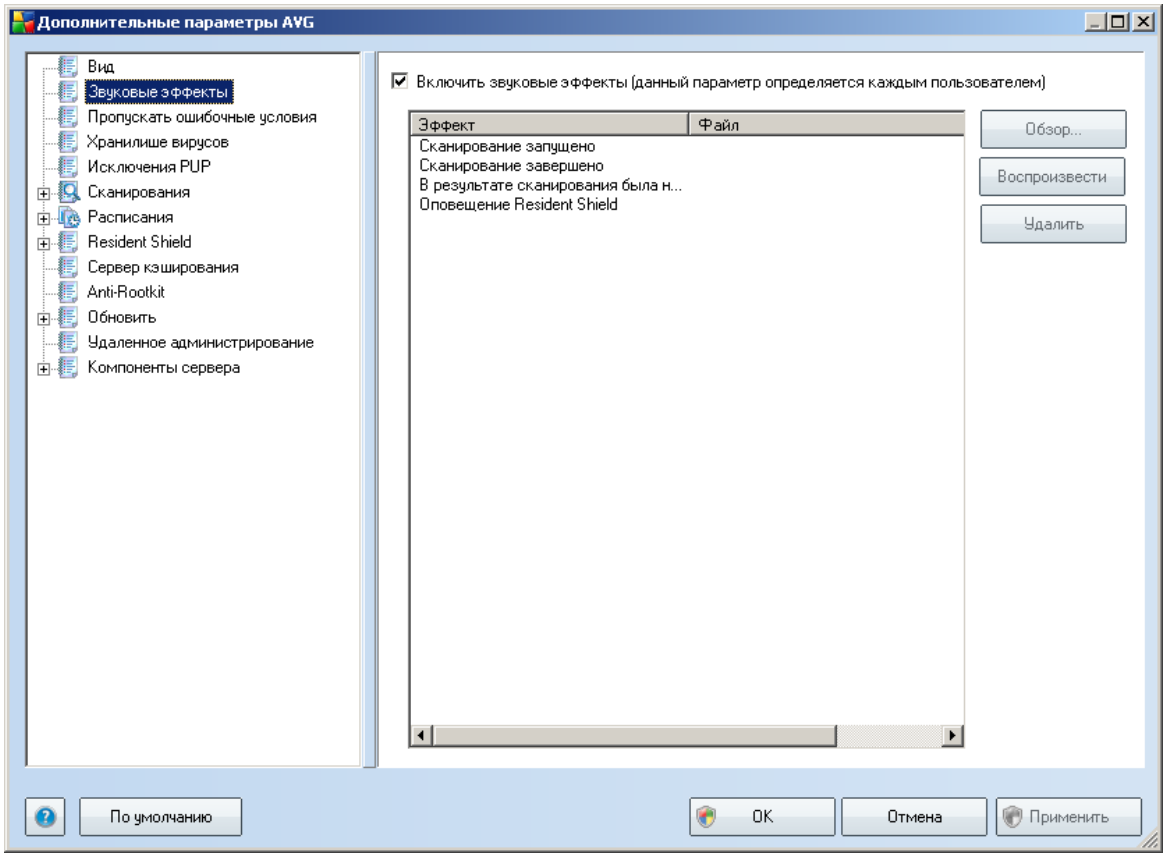
- ***Отображать уведомления о сканировании*** на панели задач. Определяет, будут ли отображаться сведения об автоматическом запуске запланированного сканирования, его состоянии и результатах.

Режим "Во время игры"

Эта функция системы AVG предназначена для полноэкранных приложений, где всплывающие окна AVG (*которые могут отображаться, например, при запуске запланированного сканирования*) способны помешать пользователю (*в результате возможно сворачивание приложения или нарушение графических параметров*). Во избежание подобных ситуаций отметьте флажком параметр ***Включить режим "Во время игры" при работе полноэкранных приложений*** (*параметр по умолчанию*).

10.2. Звуки

В окне ***Звуки*** можно указать, следует ли включить оповещение об определенных действиях AVG с помощью звуковых уведомлений. Чтобы включить эту функцию, установите флажок ***Включить звуки для событий*** (*по умолчанию отключено*), чтобы активировать список действий AVG:

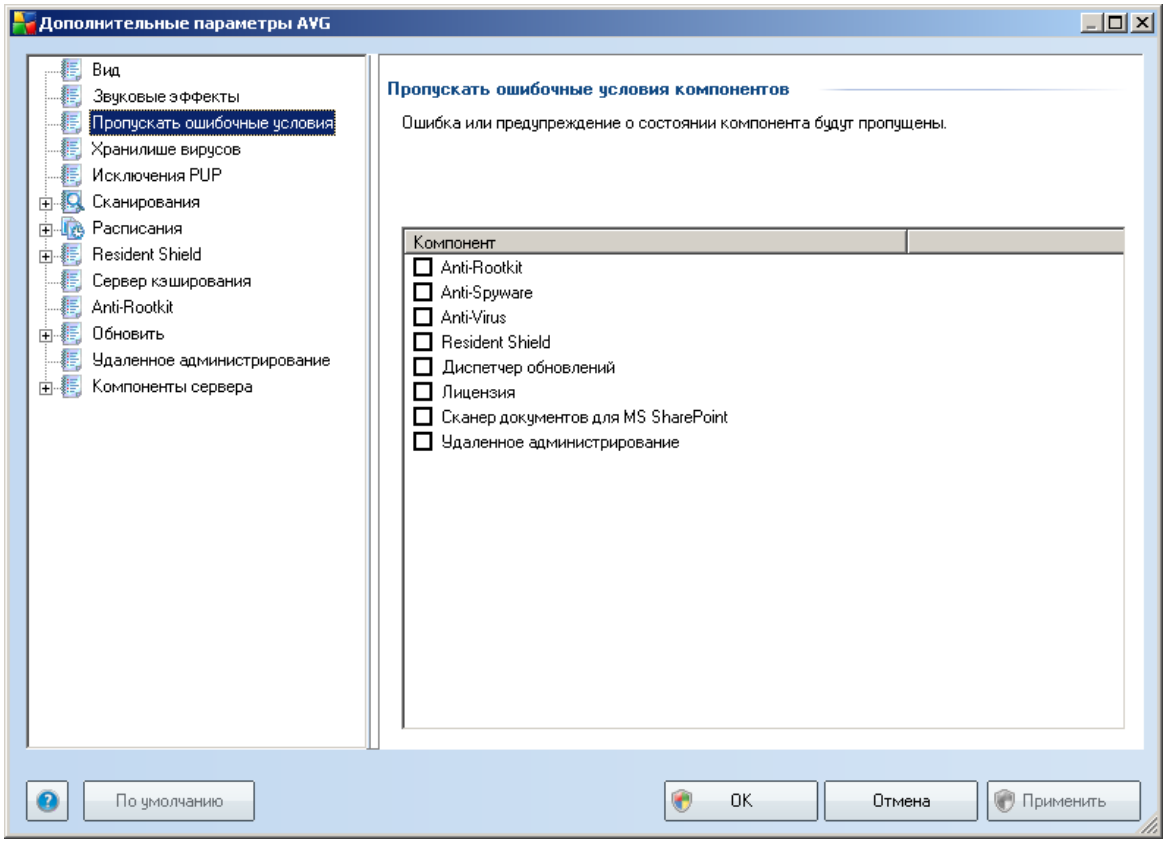


Затем выберите в списке событие и укажите (***Обзор***) на диске аудиофайл, который необходимо назначить для этого события. Чтобы прослушать выбранный аудиофайл, выделите событие в списке и нажмите кнопку ***Воспроизвести***. Чтобы удалить звук, назначенный определенному событию, нажмите кнопку ***Удалить***.

Примечание. *Поддерживаются только файлы в формате *.wav.*

10.3. Игнорирование ошибочных условий

В диалоговом окне ***Пропустить ошибочные условия компонентов*** можно отметить компоненты, о которых не требуется получать уведомления.



По умолчанию в этом списке не выбрано никаких компонентов. Это означает, что при возникновении статуса ошибки компонента сразу же появится уведомление с помощью следующих сигналов.

- ***Значок на панели задач***. Во время безупречной работы всех компонентов AVG значок имеет обычный вид; при появлении ошибок на значке появляется желтый восклицательный знак.

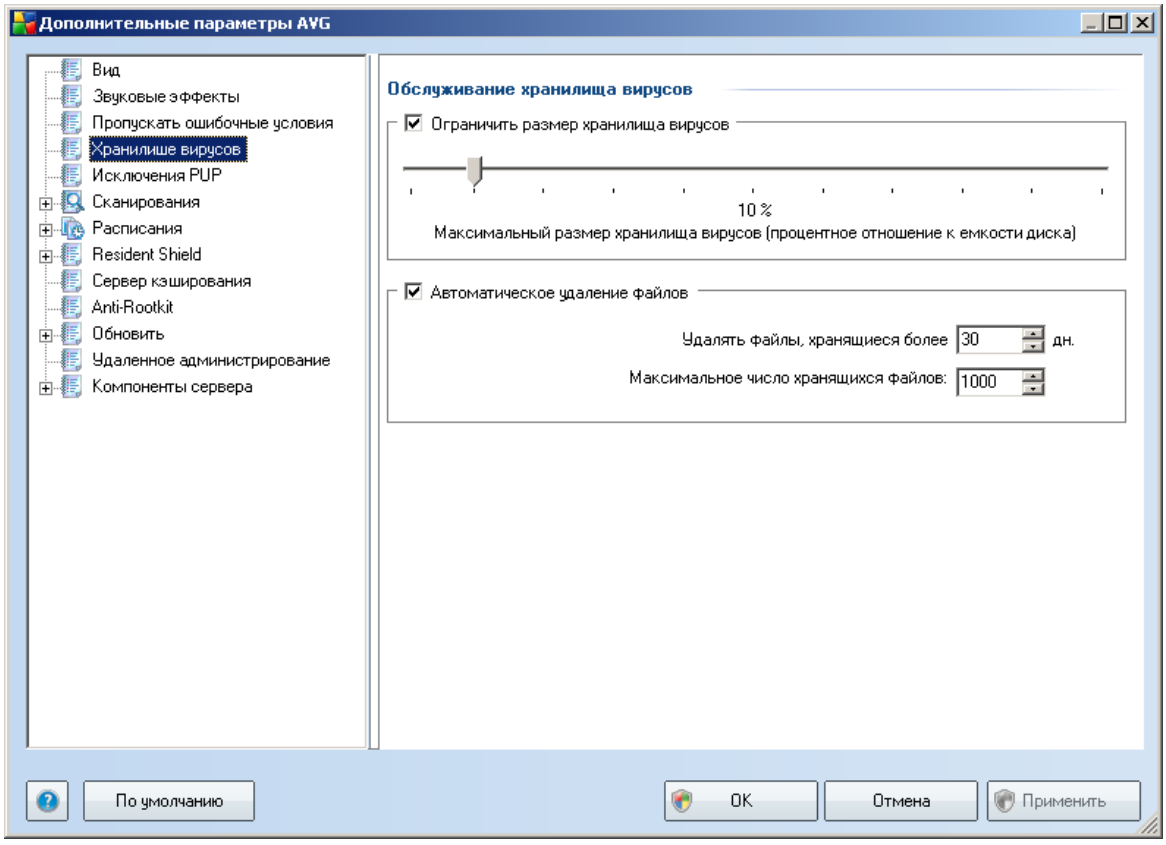
- Текстовое описание существующей проблемы в разделе ***Сведения о состоянии безопасности*** в главном окне AVG.

Может возникнуть ситуация, при которой понадобится временно отключить

компонент (*Данное действие не рекомендуется. По возможности не отключайте компоненты и не изменяйте настройки, установленные по умолчанию. Но необходимость в данном действии может возникнуть*). В данном случае значок на панели задач автоматически оповестит о состоянии ошибки компонента. Тем не менее, в данной ситуации настоящей ошибки не возникает, так как пользователь преднамеренно ее вызвал и был предварительно предупрежден о возможном риске. В то же время, если значок отображается с восклицательным знаком, он не может оповещать о дальнейших возможных ошибках.

В такой ситуации в диалоговом окне выше можно выбрать компоненты, которые могут находиться в состоянии ошибки (*или быть отключены*), и о которых не требуется получать уведомления. Этот же параметр ***Игнорирование состояния компонента*** также доступен для специальных компонентов непосредственно из обзора компонентов в главном окне AVG.

10.4. Хранилище вирусов



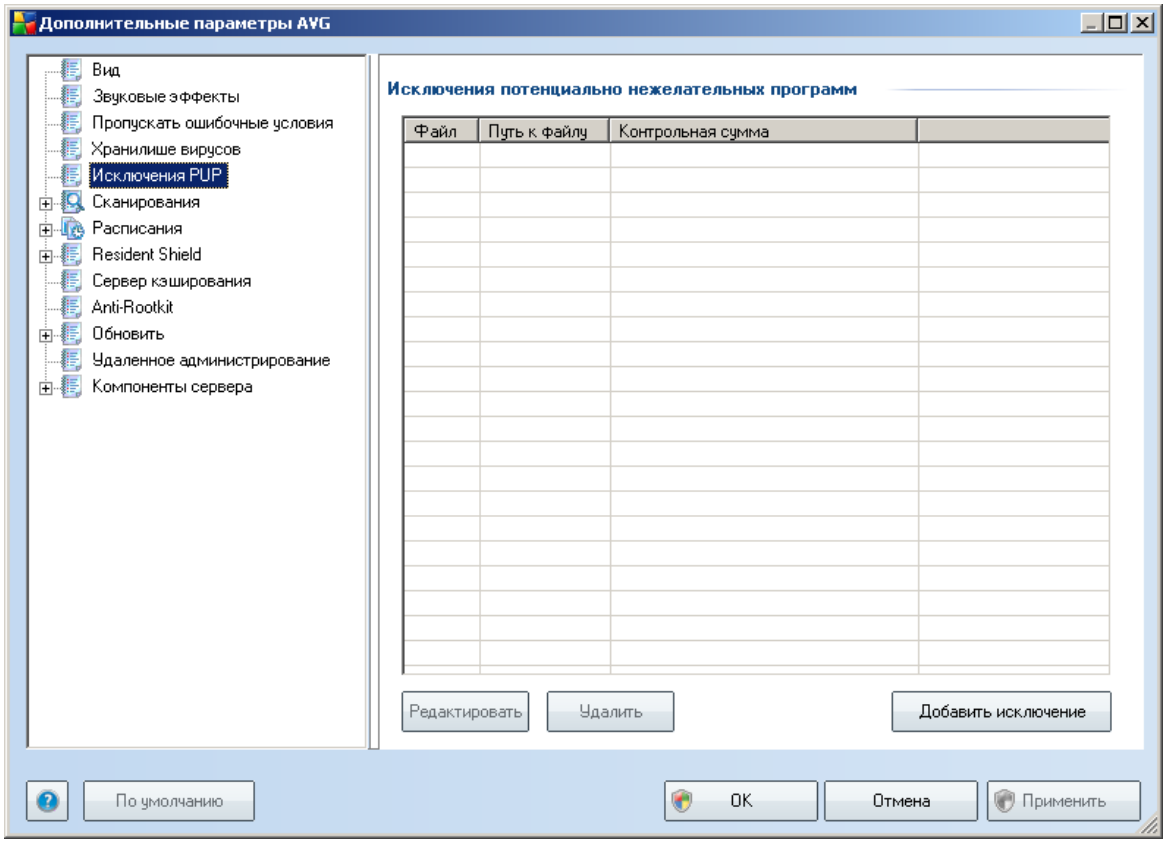
Диалоговое окно ***Обслуживание хранилища вирусов*** позволяет определить несколько параметров администрирования объектов, находящихся в ***хранилище вирусов***:

- ***Предельный размер хранилища вирусов***. Установите максимальный размер ***хранилища вирусов*** с помощью ползунка. Размер хранилища указывается пропорционально размеру локального диска.

- ***Автоматическое удаление файлов*** — в данном разделе можно указать максимальное время хранения объектов в ***хранилище вирусов*** (***Удалять файлы, хранящиеся более ... дней***), а также максимальное количество файлов, хранящихся в ***хранилище вирусов*** (***Максимальное число хранящихся файлов***)

10.5. Исключения PUP

AVG 9.0 File Server может анализировать и обнаруживать исполняемые приложения или библиотеки DLL, использование которых в системе потенциально нежелательно. В некоторых случаях пользователю может потребоваться сохранить на компьютере некоторые нежелательные программы (*программы, которые были установлены специально*). Некоторые программы, особенно бесплатные, содержат рекламное ПО. AVG может обнаружить подобное рекламное ПО и сообщить о нем, как о ***потенциально нежелательной программе***. Если необходимо сохранить подобную программу на компьютере, можно определить ее в качестве исключения потенциально нежелательной программы.



В диалоговом окне ***Исключения потенциально нежелательных программ*** отобразится список уже определенных исключений из числа потенциально нежелательных программ, которые на данный момент являются допустимыми исключениями. Список можно изменить, удалить из него существующие элементы или добавить новые исключения. О каждом исключении в списке предоставляется следующая информация.

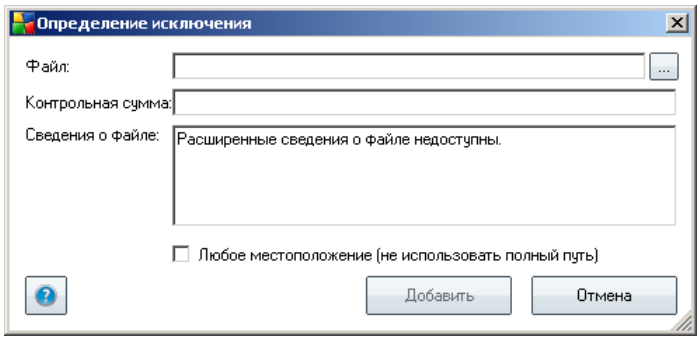
- ***Файл***. Имя соответствующего приложения.
- ***Путь к файлу***. Путь к папке приложения.
- ***Контрольная сумма***. Отображение уникальной "подписи" выбранного файла. Контрольная сумма представляет собой автоматически создаваемую строку символов, позволяющих приложению AVG безошибочно отличать выбранный файл от других. Контрольная сумма создается и отображается после успешного добавления файла.

Кнопки управления

- ***Редактировать***. Открытие диалогового окна редактирования (*соответствующего окну определения новых исключений, см. ниже*) определенного исключения, с помощью которого можно изменять параметры исключения.

- ***Удалить*** . Удаление выбранного элемента из списка исключений.

- ***Добавить исключение***. Открытие диалогового окна редактирования, с помощью которого можно определить параметры нового создаваемого исключения.



  - ***Файл***. Введите полный путь к файлу, который необходимо отметить как исключение.

  - ***Контрольная сумма***. Отображение уникальной "подписи" выбранного файла. Контрольная сумма представляет собой автоматически создаваемую строку символов, позволяющих приложению AVG безошибочно отличать выбранный файл от других. Контрольная сумма создается и отображается после успешного добавления файла.

  - ***Сведения о файле***. Отображение другой дополнительной информации о файле (*информация о лицензии или версии и т. д.*).

  - ***Любое местоположение (не использовать полный путь)***. Не устанавливайте флажок, если необходимо определить этот файл в качестве исключения только для определенного местоположения.

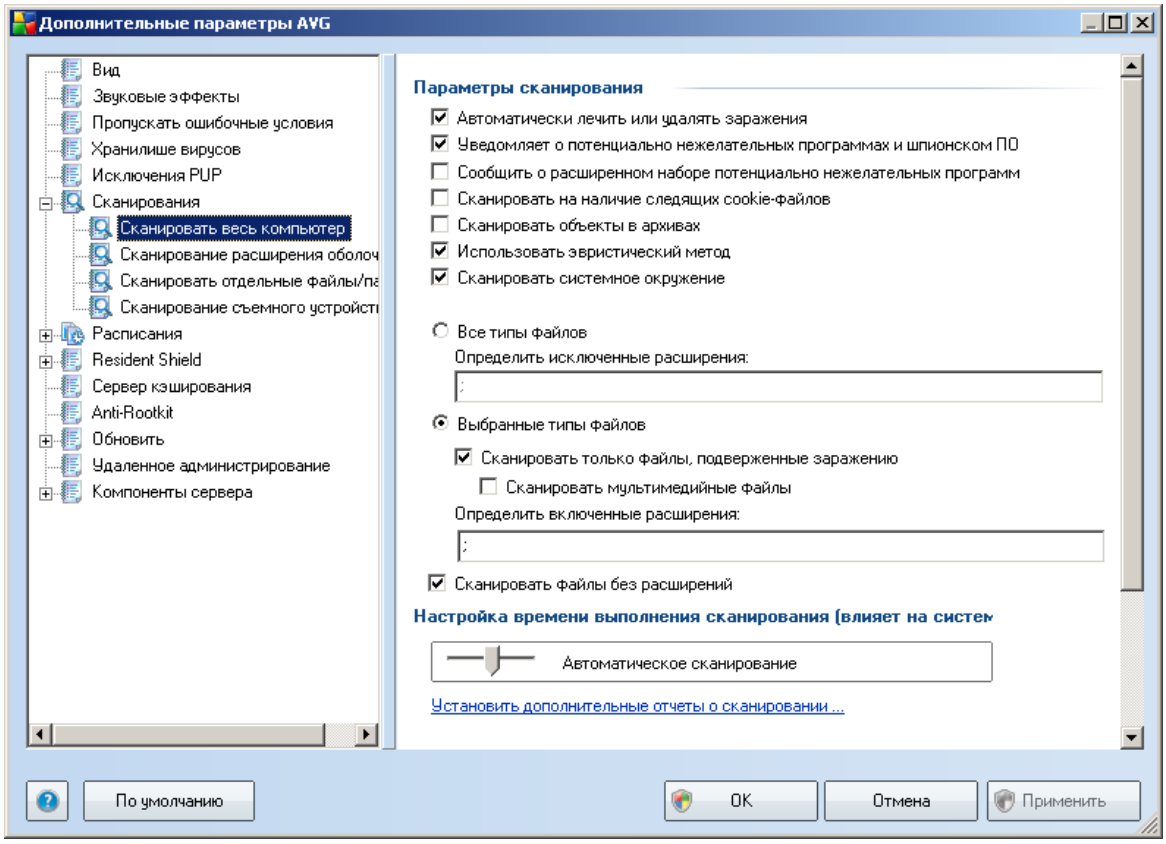
10.6. Сканирования

Дополнительные параметры сканирования разделены на четыре категории, которые относятся к особым типам сканирования, определенным поставщиком программного обеспечения.

- ***Сканирование всего компьютера***. Стандартное предварительно настроенное сканирование всего компьютера.
- ***Сканирование расширения оболочки***. Особое сканирование выбранного объекта непосредственно в среде Проводника Windows
- ***Сканирование отдельных файлов или папок***. Стандартное предварительно настроенное сканирование выбранных областей компьютера
- ***Сканирование съемного устройства***. Особое сканирование съемных устройств, подключенных к компьютеру

10.6.1. Сканирование всего компьютера

С помощью параметра ***Сканирование всего компьютера*** можно изменять параметры одного из сканирований, предварительно определенных производителем — ***сканирование всего компьютера***.



Параметры сканирования

В разделе ***Параметры сканирования*** содержатся параметры сканирования, которые можно включить или выключить при необходимости.

- ***Автоматически лечить или удалять заражения***. Обнаруженный при сканировании вирус будет вылечен автоматически, если лечение возможно. Если зараженный файл не удалось вылечить автоматически или данный параметр отключен, отобразится уведомление об обнаружении вируса с предложением выбрать действие по отношению к зараженному объекту. Рекомендуется переместить зараженный файл в хранилище вирусов.

- ***Уведомлять о потенциально нежелательных программах и угрозах появления шпионского ПО***. Данный параметр управляет функциями компонента ***Anti-Virus***, которые позволяют обнаруживать потенциально

нежелательные программы (*исполняемые файлы, которые могут работать в качестве шпионского или рекламного ПО*), блокировать их или удалять.

- ***Уведомлять о расширенном наборе потенциально нежелательных программ*** . Установите данный флажок для обнаружения расширенного пакета шпионского ПО: программы, которые полностью безопасны и не вызывают подозрений при приобретении у производителя, но могут представлять угрозу при использовании злоумышленниками. Данный параметр является дополнительной мерой, еще больше повышающей уровень безопасности, однако из-за него могут также блокироваться некоторые законные программы, поэтому по умолчанию параметр отключен;

- ***Сканировать на наличие следящих файлов cookie***. Данный параметр компонента Anti-Spyware включает сканирование системы на наличие файлов cookie (*Файлы cookie протокола HTTP используются для проверки подлинности, отслеживания и сохранения определенной информации о пользователях, например о предпочитаемых сайтах или содержимом корзин для покупок через Интернет*).

- ***Сканировать объекты в архивах***. Благодаря данному параметру при сканировании проверяются все файлы, включая файлы, хранящиеся в архивах, например ZIP, RAR и т. п.

- ***Использовать эвристический анализ***. Эвристический анализ (*динамичная эмуляция команд сканированных объектов в виртуальной компьютерной среде*) является одним из способов, используемых для выявления вирусов при сканировании.

- ***Сканировать системную среду***. При сканировании будут также проверяться системные области компьютера.

Далее необходимо выбрать файлы для сканирования

- ***Все типы файлов*** с возможностью определения исключений из сканирования посредством предоставления списка расширений файлов, разделенных запятыми, сканирование которых проводиться не будет.

- ***Выбранные типы файлов***. Можно указать сканирование только тех файлов, которые подвержены заражению (*файлы, не подверженные заражению, не будут сканироваться, например простые текстовые файлы или другие неисполняемые файлы*), включая мультимедийные файлы (*видео- и аудиофайлы — если не устанавливать этот флажок, время сканирования значительно уменьшится, так как эти файлы обладают довольно большим размером и вероятность их заражения вирусом мала*).

С помощью расширений можно указать файлы, которые необходимо сканировать всегда.

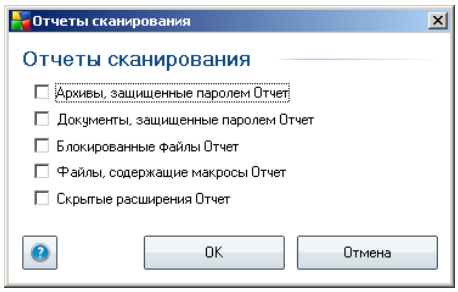
- Дополнительно можно установить флажок ***Сканировать файлы без расширений***. Он установлен по умолчанию. Рекомендуется не изменять его без веских причин. Файлы без расширения являются подозрительными, поэтому необходимо выполнять их сканирование каждый раз.

Приоритет процесса сканирования

В разделе ***Приоритет процесса сканирования*** можно дополнительно выбрать необходимую скорость сканирования в зависимости от использования системных ресурсов. По умолчанию для данного параметра установлено значение среднего уровня автоматического использования ресурсов. Если необходимо, чтобы сканирование выполнялось быстрее, это займет меньше времени, но во время этого процесса будет значительно увеличено использование системных ресурсов, что снизит производительность других процессов, выполняемых на компьютере (*этот параметр можно включить, если компьютер включен, но не используется*). И наоборот, можно снизить уровень использования системных ресурсов с помощью увеличения продолжительности сканирования.

Установить дополнительные отчеты о сканировании ...

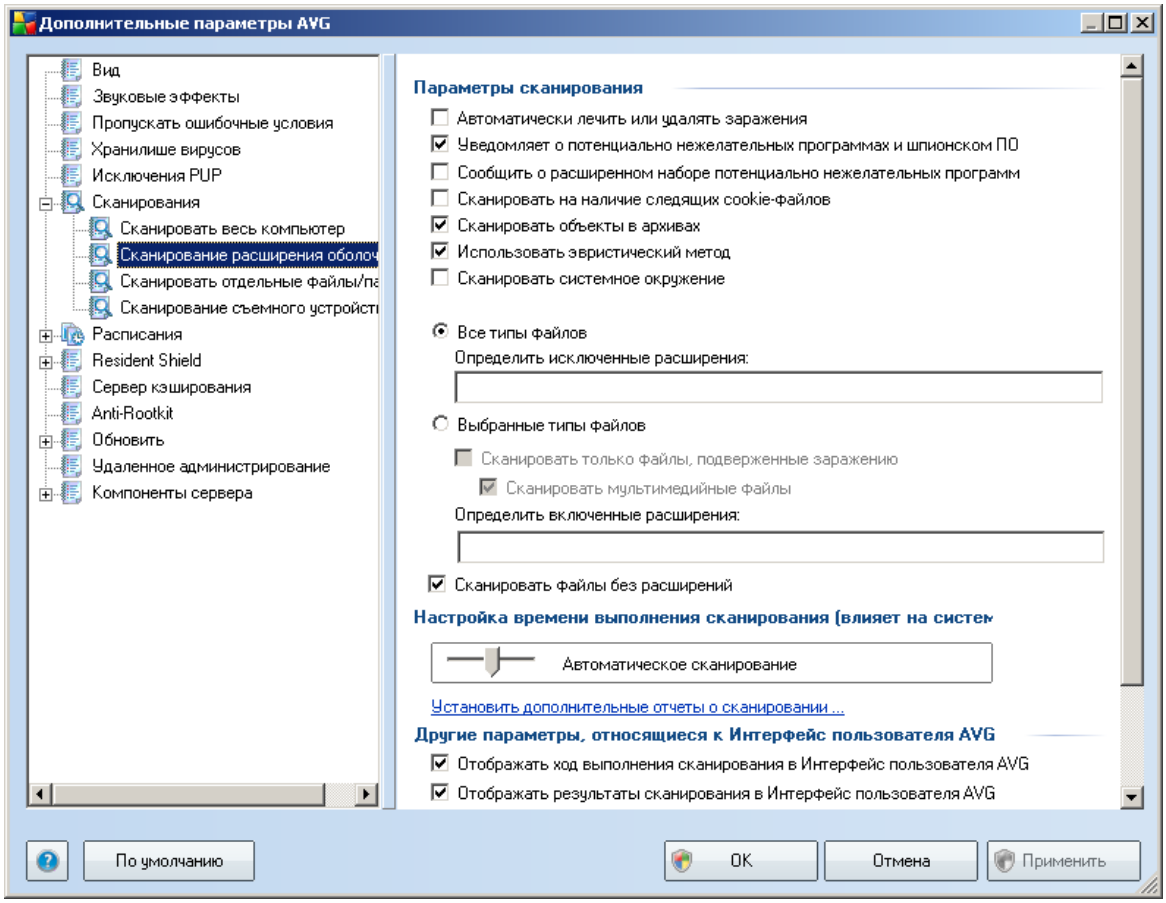
Щелкните ссылку ***Настроить дополнительные отчеты сканирования ...***, чтобы открыть диалоговое окно ***Отчеты сканирования***, в котором можно выбрать типы объектов, о которых буду выводиться отчеты при сканировании.



10.6.2. Сканирование расширения оболочки

Как и предыдущий элемент ***Сканировать весь компьютер***, элемент ***Сканирование расширения оболочки*** также содержит несколько предварительно установленных поставщиком ПО параметров для настройки

сканирования. Данные параметры предназначены для настройки сканирования определенных объектов, запускаемых непосредственно из Проводника Windows (*расширение оболочки*), см. раздел ***Сканирование в Проводнике Windows***.



Список параметров соответствует параметрам элемента ***Сканирование всего компьютера***. Однако параметры по умолчанию отличаются. Для элемента ***Сканировать весь компьютер*** большинство параметров установлено, а для элемента ***Сканирование расширения оболочки*** (***Сканирование в Проводнике Windows***) установлены только подходящие параметры.

Примечание. *Описание специальных параметров приведено в разделе* ***Расширенные параметры AVG/Сканирования/Сканирование всего компьютера***.

Однако существуют некоторые параметры, которые отображаются только при сканировании расширения оболочки. Эти параметры приведены ниже (и описаны в

разделе **Другие параметры, связанные с интерфейсом пользователя AVG**).

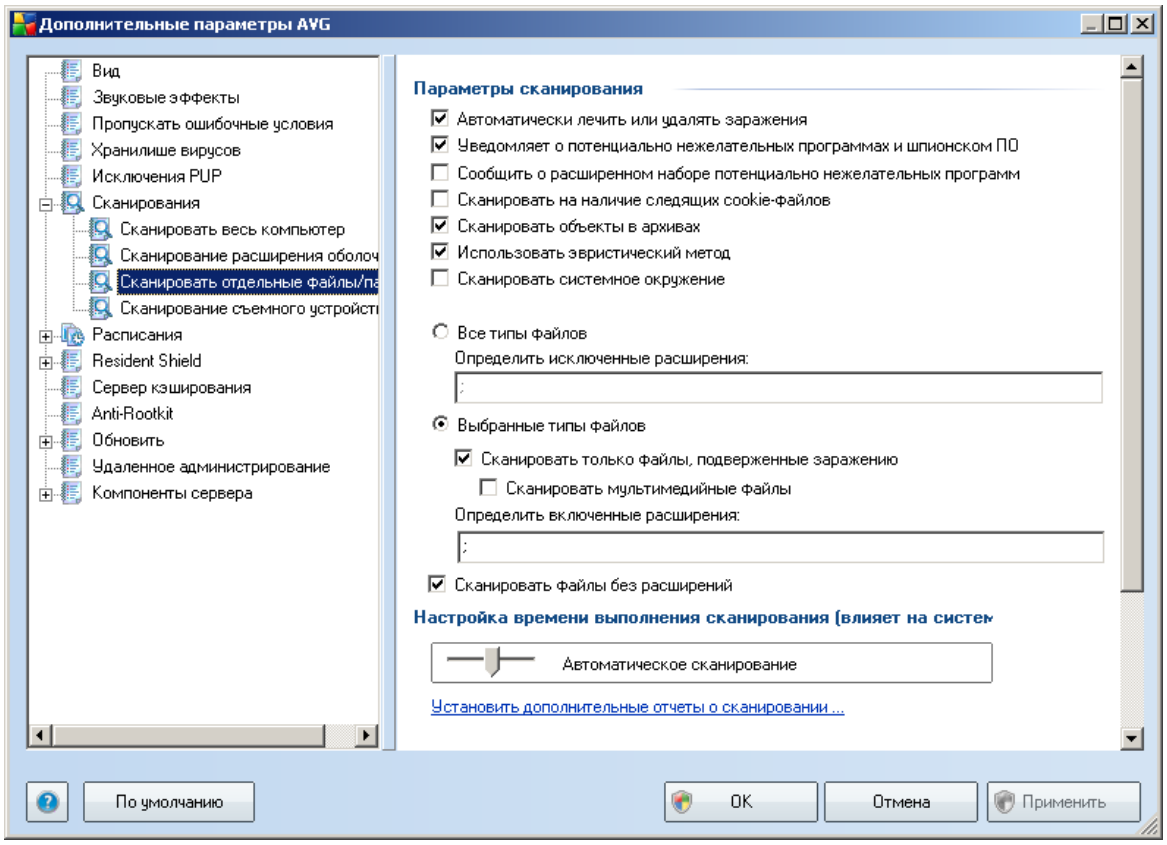
- ***Отображать ход выполнения сканирования в интерфейсе пользователя AVG***. Если этот флажок установлен, будет отображаться уведомление о каждом запуске и завершении сканирования расширения оболочки (в нижнем правом углу экрана будет появляться небольшое информационное сообщение).

- ***Отображать результаты сканирования в интерфейсе пользователя AVG***. Если этот флажок установлен, при завершении сканирования расширения оболочки будет открываться интерфейс пользователя AVG и стандартное диалоговое окно ***Сведения о результатах сканирования*** (количество вкладок будет зависеть от результатов сканирования).

    - ***Только если результаты сканирования содержат угрозы***. Этот элемент активен, если установлен предыдущий флажок. Когда он выбран, диалоговое окно ***Сведения о результатах сканирования*** будет отображаться только в том случае, если во время сканирования расширения оболочки были обнаружены какие-либо угрозы.

10.6.3. Сканирование отдельных файлов или папок

Интерфейс редактирования ***Сканировать отдельные файлы или папки*** полностью соответствует диалоговому окну редактирования ***Сканировать весь компьютер***. Все параметры конфигурации также не отличаются; однако параметры по умолчанию являются более строгими при ***сканировании всего компьютера***:

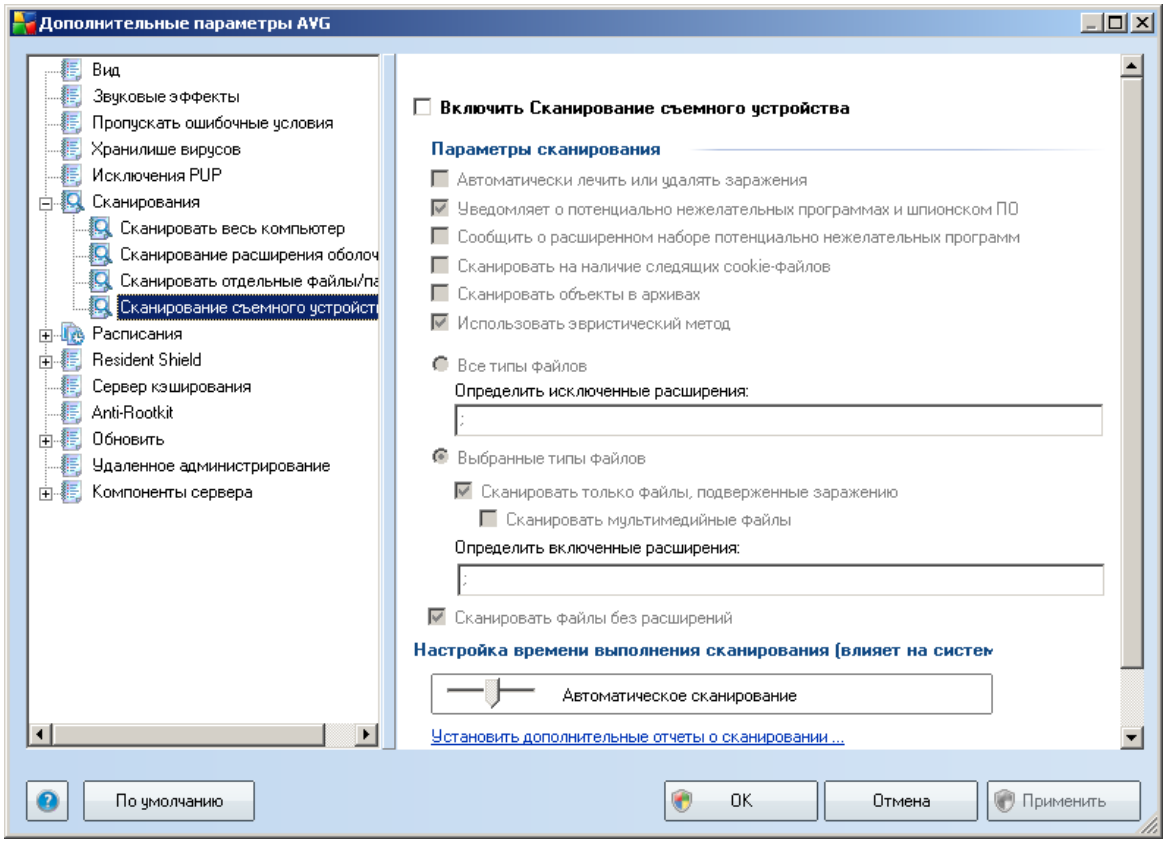


Все параметры, настроенные в этом диалоговом окне конфигурации, применяются только в выбранным для сканирования областям с помощью ***Сканирование определенных файлов или папок***!

Примечание. *Описание специальных параметров приведено в главе* ***Расширенные настройки AVG/Сканирования/Сканирование всего компьютера***.

10.6.4. Сканирование съемного устройства

Свойства интерфейса редактирования параметров диалогового окна ***Сканирование съемного устройства*** соответствуют свойствам редактирования параметров диалогового окна ***Сканирование всего компьютера***.



Диалоговое окно ***Сканирование съемного устройства*** открывается автоматически после подключения съемного устройства к компьютеру. По умолчанию сканирование отключено. Однако очень важно сканировать съемные устройства на наличие потенциальных угроз, так как они являются основным источником заражений. Чтобы данное сканирование запускалось автоматически, установите флажок ***Включить сканирование съемного устройства***.

Примечание. *Описание специальных параметров приведено в главе* ***Расширенные настройки AVG/Сканирования/Сканирование всего компьютера***.

10.7. Расписания

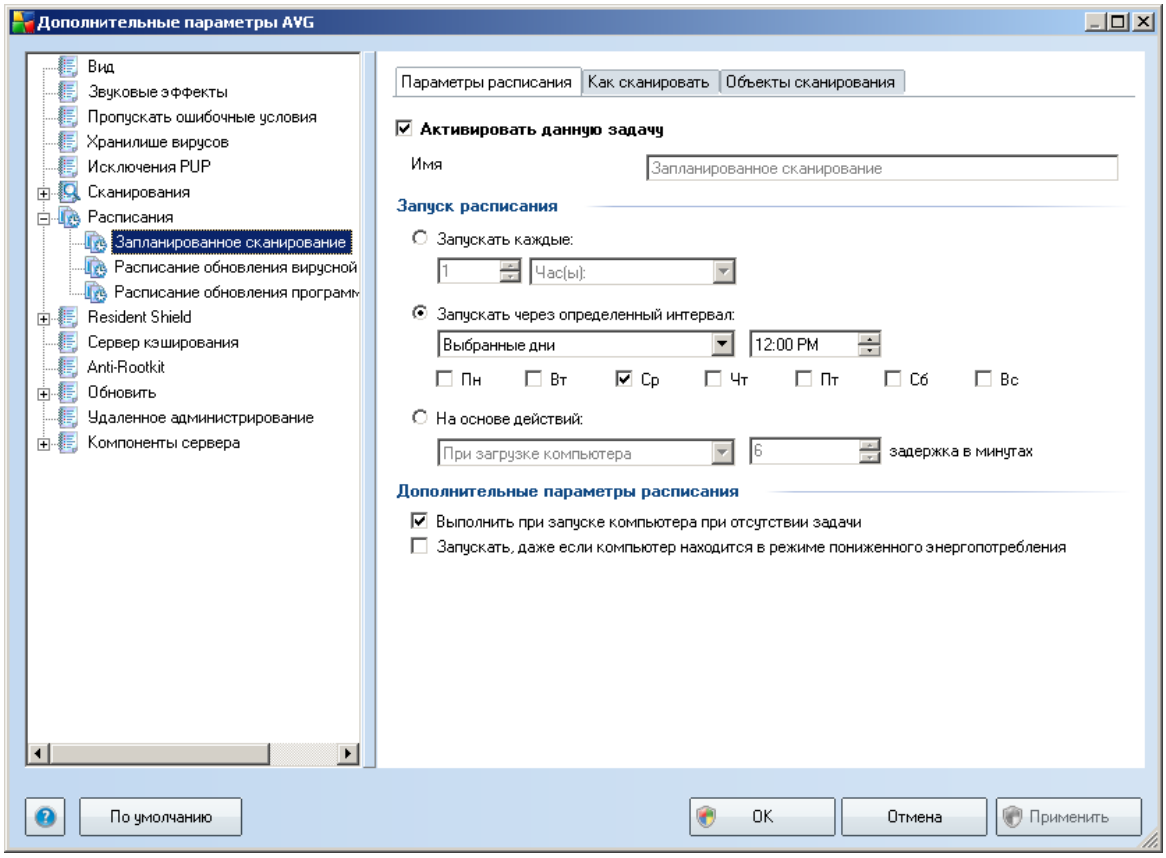
Раздел ***Расписания*** позволяет изменить стандартные настройки расписания.

- Расписание сканирования всего компьютера.

- Расписание обновления вирусной базы данных
- Расписание обновления программы

10.7.1. Запланированное сканирование

С помощью следующих трех вкладок можно изменить параметры запланированного сканирования (*или создать новое расписание*).



На вкладке ***Параметры расписания*** можно сначала установить или снять флажок ***Активировать данную задачу***, чтобы временно отключить запланированную проверку и включить ее при необходимости.

В текстовом поле ***Имя*** (*неактивном для всех расписаний по умолчанию*) отображается имя, назначенное данному расписанию поставщиком программы. Для новых расписаний (*чтобы добавить новое расписание, щелкните правой*

кнопкой мыши элемент ***Запланированное сканирование*** *в левом навигационном дереве*) можно указать собственное имя. При этом текстовое поле будет доступно для редактирования. Старайтесь использовать краткие, содержательные и понятные названия сканирований, так как позже это облегчит их поиск среди остальных сканирований.

Пример. *Названия "Новое сканирование" или "Мое сканирование" не являются содержательными, так как не связаны с объектами, которые будут проверяться. И наоборот, название "Сканирование системных областей" является хорошим содержательным названием. Хотя и не обязательно указывать в названии сканирования, является ли оно сканированием всего компьютера или только сканированием выбранных файлов или папок, созданные сканирования будут определяться как разновидности сканирования выбранных файлов и папок.*

В данном диалоговом окне можно определить следующие параметры сканирования.

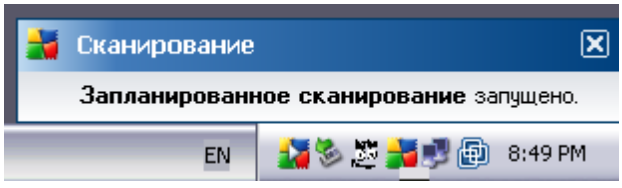
Выполняемое расписание

Здесь можно указать временные интервалы запуска нового запланированного сканирования. Можно определить время запуска сканирования через определенные промежутки времени (***Запускать каждые ...***), указать точные дату и время запуска сканирования (***Запускать в определенное время ...***), а также определить событие, с которым должен быть связан запуск сканирования (***Действие связано с включением компьютера***).

Дополнительные параметры расписания

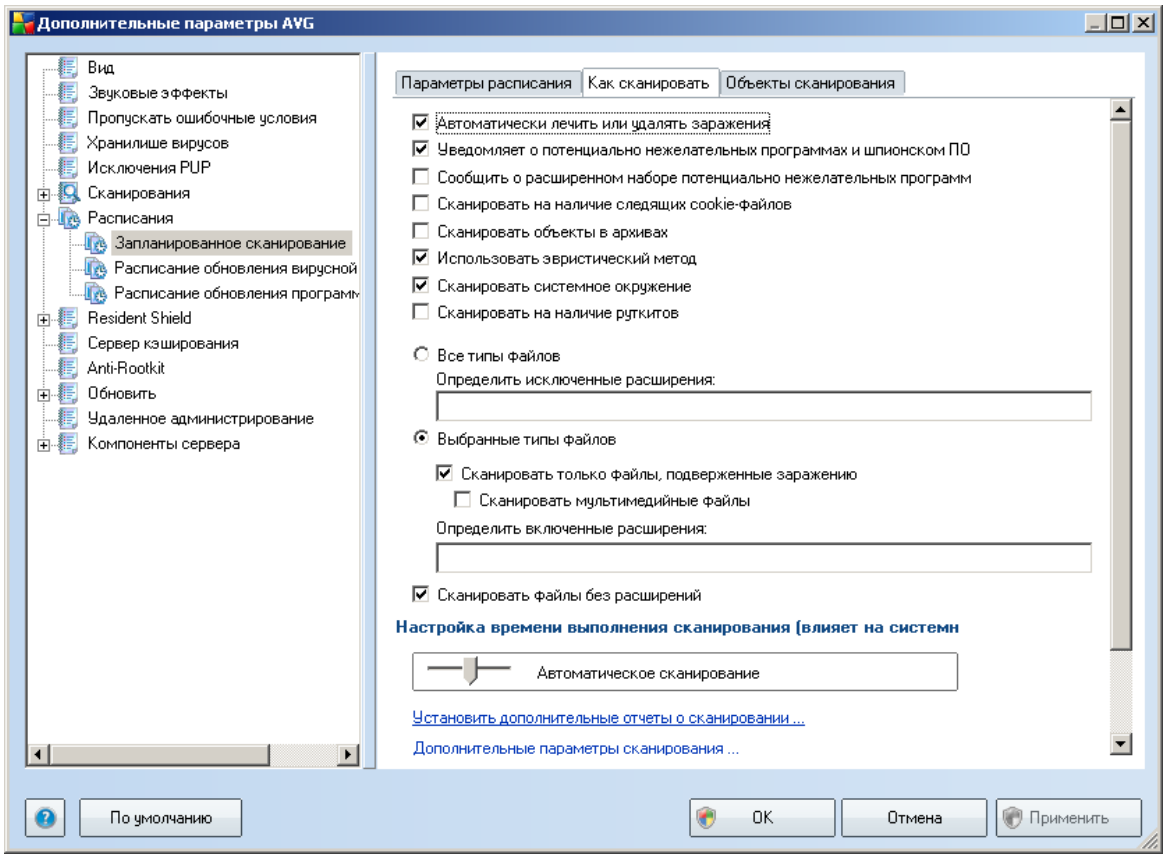
Данный раздел позволяет определить условия, при которых должен или не должен выполняться запуск сканирования, если компьютер работает в энергосберегающем режиме или выключен.

После запуска обновления в указанное время появится всплывающее окно с уведомлением о данном событии над значком AVG на панели задач.



Затем появится новый значок AVG на панели задач (*цветной значок с белой*

стрелкой — см. изображение выше), сообщающий о том, что запланированное сканирование запущено.



На вкладке ***Способ сканирования*** приведен список параметров сканирования, которые при необходимости можно включить или отключить. По умолчанию большинство параметров включены и используются при сканировании. Если нет веских оснований для изменения данных параметров, рекомендуется не изменять стандартную конфигурацию.

- ***Автоматически лечить или удалять заражения*** . (*Включено по умолчанию*). Обнаруженный при сканировании вирус будет вылечен автоматически, если лечение возможно. Если зараженный файл не удалось вылечить автоматически или данный параметр отключен, отобразится уведомление об обнаружении вируса с запросом выбрать действие по отношению к зараженному объекту. Рекомендуется переместить зараженный файл в хранилище вирусов.

- ***Сообщать о потенциально нежелательных программах и шпионском ПО***. (*Включено по умолчанию*). Данный параметр управляет работой компонента Anti-Virus, который позволяет обнаруживать потенциально нежелательные программы (*исполняемые файлы, которые могут работать в качестве шпионского или вредоносного ПО*), блокировать их или удалять.

- ***Уведомлять о расширенном наборе потенциально нежелательных программ***. (*Отключено по умолчанию*). Этот параметр обеспечивает обнаружение расширенного пакета шпионского ПО: программы, которые полностью безопасны и не вызывают подозрений при приобретении у производителя, но могут представлять угрозу при использовании злоумышленниками. Данный параметр является дополнительной мерой, еще больше повышающей уровень безопасности, однако из-за него могут также блокироваться некоторые законные программы, поэтому по умолчанию параметр отключен.

- ***Сканировать на наличие следящих файлов cookie***. (*Отключено по умолчанию*). Благодаря данному параметру компонента Anti-Spyware программа сканирует систему на наличие файлов cookie (Файлы cookie HTTP используются для проверки подлинности, отслеживания и сохранения определенной информации о пользователях, например о предпочитаемых сайтах или содержимом корзин для покупок через Интернет))

- ***Сканировать объекты в архивах***. (*Отключено по умолчанию*). В случае выбора данного параметра при сканировании будут проверяться все файлы, включая файлы, хранящиеся в архивах, например ZIP, RAR и т. п.

- ***Использовать эвристический анализ***. (*Включено по умолчанию*). Эвристический анализ (*динамичная эмуляция команд сканированных объектов в среде виртуального компьютера*) является одним из способов, используемых для обнаружения вирусов при сканировании.

- ***Сканировать системную среду***. (*Включено по умолчанию*). При сканировании также будут проверены системные области компьютера.

- ***Сканировать на наличие rootkits***. Установите этот флажок, чтобы искать rootkits при сканировании всего компьютера. Определение средств rootkit можно выполнить отдельно с помощью компонента ***Anti-Rootkit***.

Далее необходимо выбрать файлы для сканирования

- ***Все типы файлов*** с возможностью определения исключений из сканирования посредством предоставления списка расширений файлов, разделенных запятыми, сканирование которых проводиться не будет.

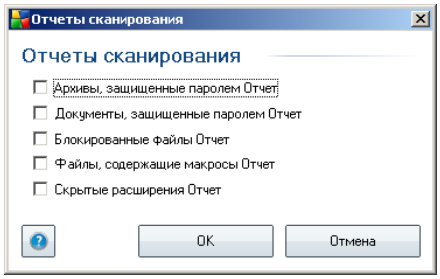
- ***Выбранные типы файлов***. Можно указать сканирование только тех файлов, которые подвержены заражению (*файлы, не подверженные заражению, не будут сканироваться, например простые текстовые файлы или другие неисполняемые файлы*), включая мультимедийные файлы (*видео- и аудиофайлы — если не устанавливать этот флажок, время сканирования значительно уменьшится, так как эти файлы обладают довольно большим размером и вероятность их заражения вирусом мала*). С помощью расширений можно указать файлы, которые необходимо сканировать всегда.

- Дополнительно можно установить флажок ***Сканировать файлы без расширений***. Он установлен по умолчанию. Рекомендуется не изменять его без веских причин. Файлы без расширения являются подозрительными, поэтому необходимо выполнять их сканирование каждый раз.

Приоритет процесса сканирования

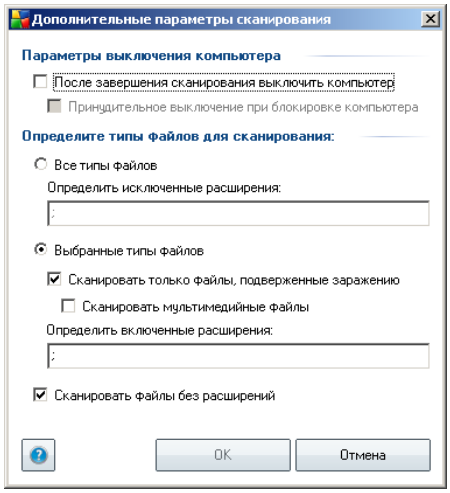
В разделе ***Приоритет процесса сканирования*** можно дополнительно выбрать необходимую скорость сканирования в зависимости от использования системных ресурсов. По умолчанию для данного параметра установлено значение среднего уровня автоматического использования ресурсов. Если необходимо, чтобы сканирование выполнялось быстрее, это займет меньше времени, но во время этого процесса будет значительно увеличено использование системных ресурсов, что снизит производительность других процессов, выполняемых на компьютере (*этот параметр можно включить, если компьютер включен и не используется*). И наоборот, можно снизить уровень использования системных ресурсов с помощью увеличения продолжительности сканирования.

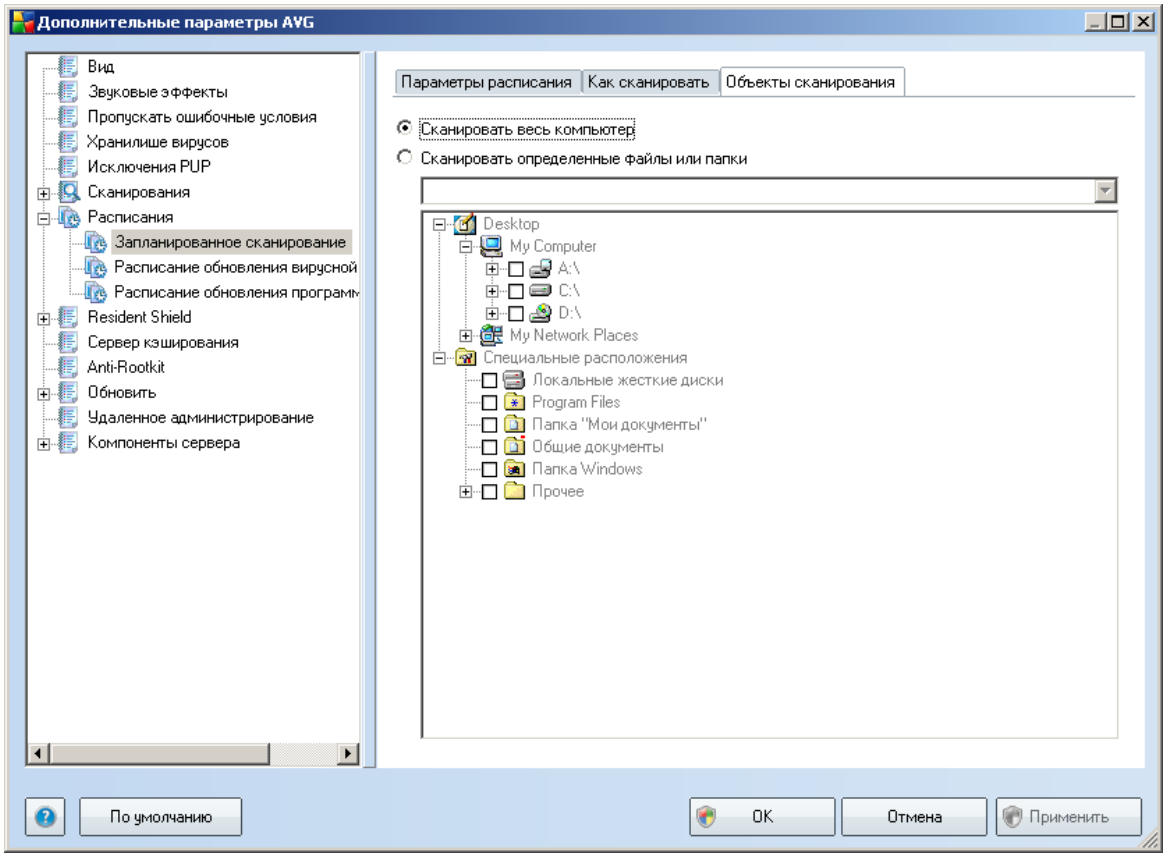
Щелкните ссылку ***Настроить дополнительные отчеты сканирования ...***, чтобы открыть диалоговое окно ***Отчеты сканирования***, в котором можно выбрать типы объектов, о которых буду выводиться отчеты при сканировании.



Щелкните ссылку ***Дополнительные параметры сканирования ...***, чтобы открыть новое диалоговое окно ***Параметры выключения компьютера***, с

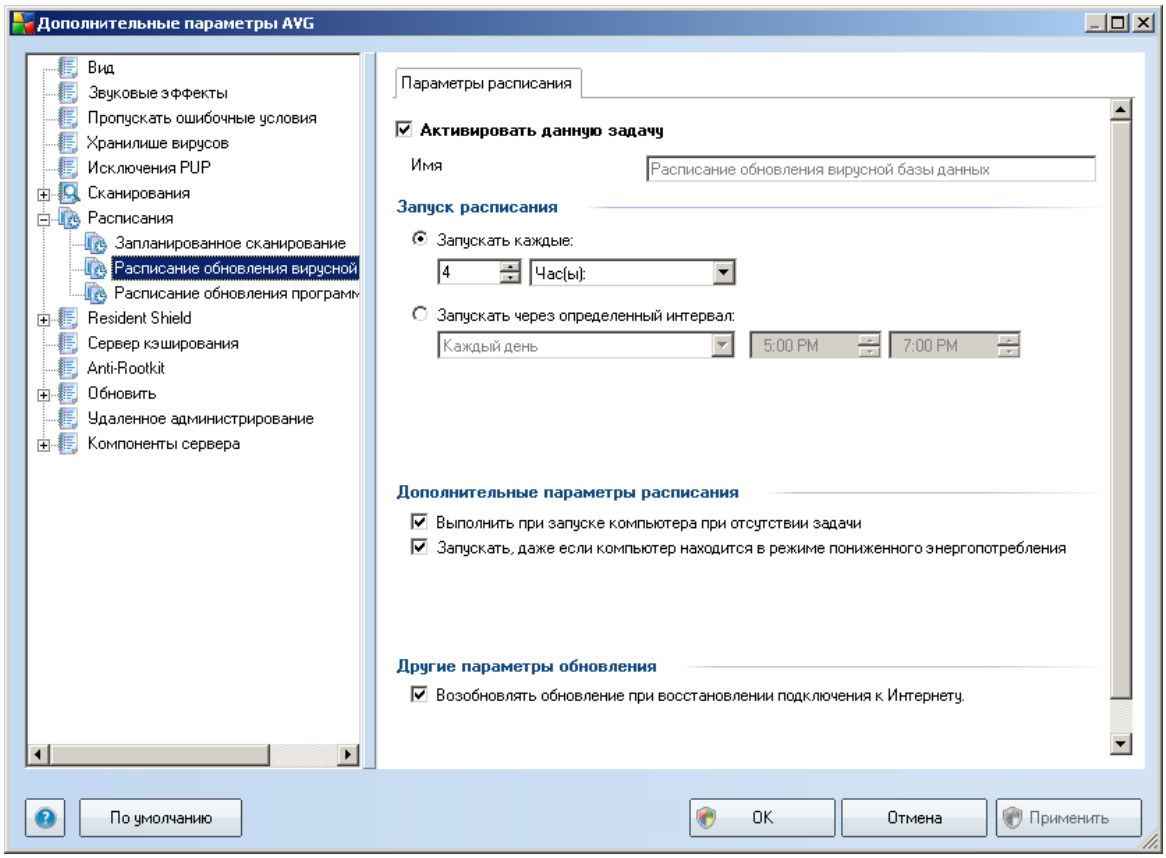
помощью которого можно настроить автоматическое выключение компьютера после завершения процесса сканирования. После выбора этого параметра (***Выключить компьютер после завершения сканирования***) становится доступен новый параметр, позволяющий выключать компьютер, даже если он заблокирован (***Принудительное выключение при блокировке компьютера***).





На вкладке ***Объекты сканирования*** можно запланировать сканирование всего компьютера или сканирование отдельных файлов и папок. Если выбрать сканирование определенных файлов и папок, в нижней части этого диалогового окна станет активна отображаемая древовидная структура, в которой можно указать сканируемые папки.

10.7.2. Расписание обновления вирусной базы данных



На вкладке ***Параметры расписания*** можно сначала установить или снять флажок ***Активировать данную задачу***, чтобы временно отключить запланированное обновление вирусной базы данных, и включить его снова при необходимости.

Основное расписание обновления вирусной базы данных может быть настроено с помощью компонента ***Диспетчер обновления***. В данном диалоговом окне могут быть настроены параметры расписания обновления вирусной базы данных:

В текстовом поле ***Имя*** (*неактивном для всех расписаний по умолчанию*) отображается имя, назначенное данному расписанию поставщиком программы. Для новых расписаний (*чтобы добавить новое расписание, щелкните правой кнопкой мыши элемент* ***Расписание обновления вирусной базы данных*** *в левом дереве навигации*) можно указать собственное имя. Текстовое поле будет доступно для редактирования. Старайтесь использовать краткие, содержательные

и точные имена расписаний, так как в дальнейшем это облегчит работу с ними.

Выполняемое расписание

В этом разделе необходимо указать временные интервалы для запланированного запуска обновления вирусной базы данных. Можно определить время запуска обновления через определенные промежутки времени (***Запускать каждые...***), указать точные дату и время запуска (***Запускать в определенное время...***) или определить событие, с которым должен быть связан запуск обновления (***Действие связано с включением компьютера***).

Дополнительные параметры расписания

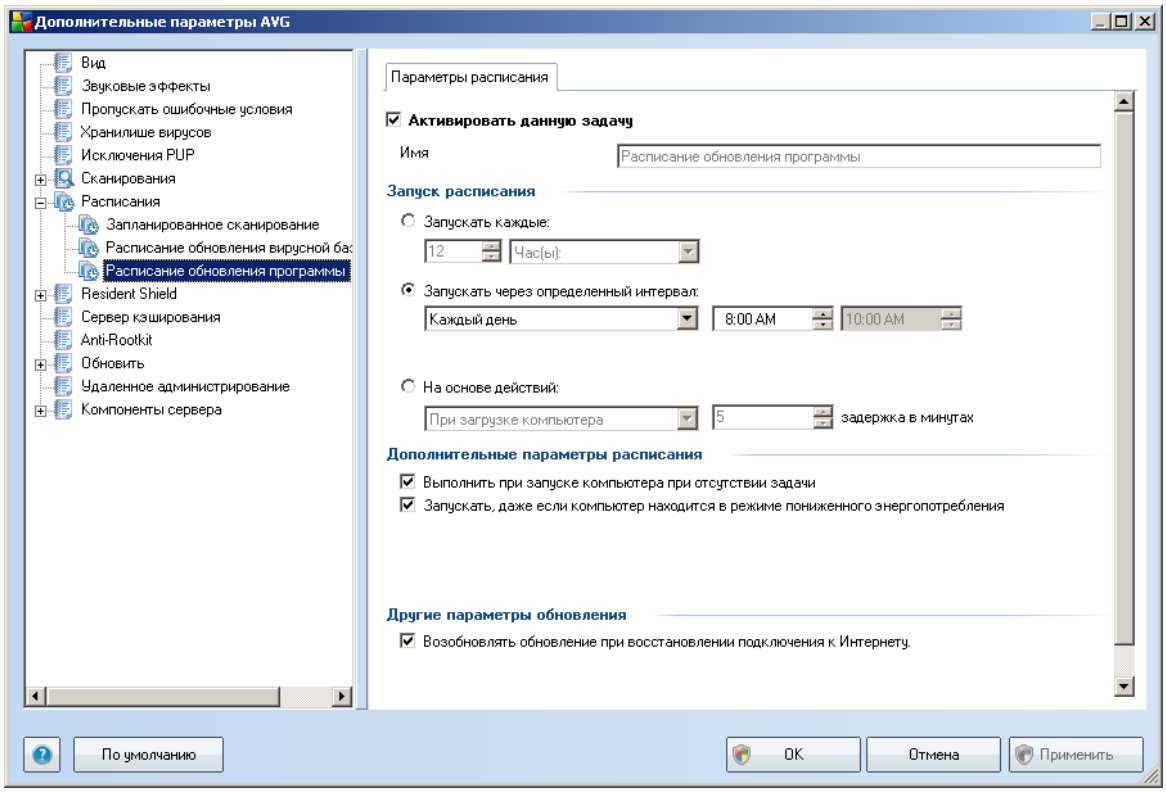
Данный раздел позволяет определить условия, при которых должен или не должен выполняться запуск обновления вирусной базы данных, если компьютер работает в энергосберегающем режиме или выключен.

Другие параметры обновления

Установите флажок ***Возобновлять обновление при восстановлении подключения к Интернету***, чтобы в случае разрыва соединения с Интернетом и при сбое процесса обновления компонента процесс запускался сразу же после восстановления подключения к Интернету.

После запуска запланированного обновления отображается всплывающее окно с уведомлением о данном событии над значком AVG на панели задач (*если параметры по умолчанию диалогового окна* ***Дополнительные параметры/ Внешний вид*** *не были изменены)*.

10.7.3. Расписание обновления программы



На вкладке ***Параметры расписания*** можно сначала установить или снять флажок ***Активировать данную задачу*** для временного отключения обновления программы или его повторного включения при необходимости.

В текстовом поле ***Имя*** (*неактивном для всех расписаний по умолчанию*) отображается имя, назначенное данному расписанию поставщиком программы. Для новых расписаний (*чтобы добавить новое расписание, щелкните правой кнопкой мыши элемент* ***Расписание обновления программы*** *в левом дереве навигации*) можно указать собственное имя. При этом текстовое поле будет доступно для редактирования. Старайтесь использовать краткие, содержательные и точные имена расписаний, так как в дальнейшем это облегчит работу с ними.

Выполняемое расписание

Укажите временные интервалы для запуска нового запланированного обновления программы. Можно определить время запуска обновления через определенные

промежутки времени (***Запускать каждые...***), указать точные дату и время запуска (***Запускать в определенное время...***) или определить событие, с которым должен быть связан запуск обновления (***Действие связано с включением компьютера***).

Дополнительные параметры расписания

Данный раздел позволяет определить условия, при которых должен или не должен выполняться запуск обновления программы, если компьютер работает в энергосберегающем режиме или выключен.

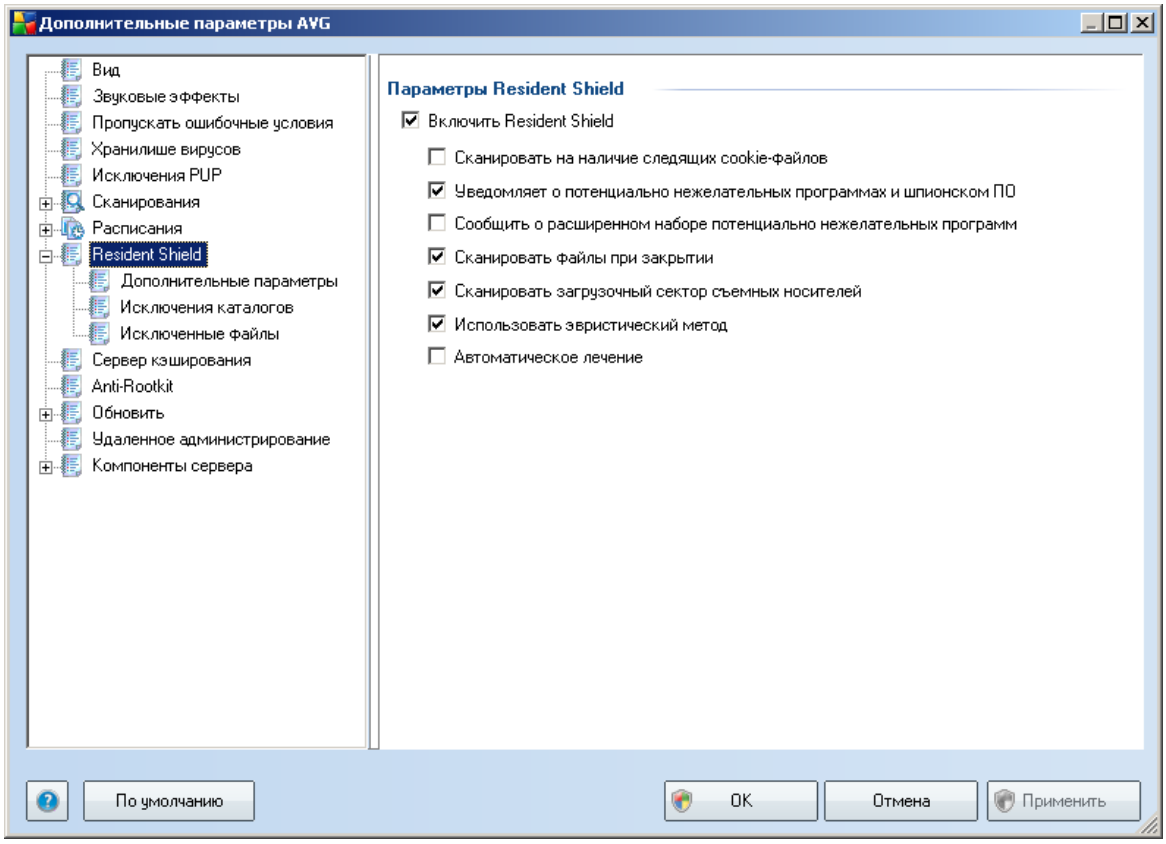
Другие параметры обновления

Установите флажок ***Возобновлять обновление при восстановлении подключения к Интернету***, чтобы в случае разрыва соединения с Интернетом и сбое процесса обновления компонента процесс запускался сразу же после восстановления подключения к Интернету.

После запуска запланированного обновления отображается всплывающее окно с уведомлением о данном событии над значком AVG на панели задач (*если параметры по умолчанию диалогового окна* ***Дополнительные параметры/ Внешний вид*** *не были изменены)*.

10.8. Resident Shield

Компонент ***Resident Shield*** обеспечивает защиту в режиме реального времени файлов и папок от вирусов, шпионского ПО и других разновидностей вредоносного ПО.



В диалоговом окне ***Параметры Resident Shield*** можно включить или отключить защиту, осуществляемую компонентом ***Resident Shield***, установив или сняв флажок с параметра ***Включить Resident Shield*** (*по умолчанию данный параметр включен*). Также можно выбрать функции компонента ***Resident Shield***, которые необходимо активировать.

- ***Сканировать на наличие следящих файлов cookie***. Данный параметр определяет обнаружение файлов cookie при сканировании. (*Файлы cookie протокола HTTP используются для проверки подлинности, отслеживания и сбора определенной информации о пользователях, например о предпочитаемых сайтах или содержимом корзин для покупок в Интернете*).

- ***Уведомлять о потенциально нежелательных программах и угрозах появления шпионского ПО***. (*Отключен по умолчанию*). Сканирование на наличие потенциально нежелательного ПО (*исполняемых приложений, которые могут функционировать как разновидности шпионского или рекламного ПО*).

- ***Уведомлять о расширенном наборе потенциально нежелательных***

программ. (*Отключен по умолчанию*). Обнаружение расширенного пакета шпионского ПО: программы, которые полностью безопасны и не вызывают подозрений при приобретении у производителя, но могут представлять угрозу при использовании злоумышленниками. Данный параметр является дополнительной мерой, еще больше повышающей уровень безопасности, однако из-за него могут также блокироваться некоторые законные программы, поэтому по умолчанию параметр отключен.

- ***Сканировать файлы при закрытии***. Сканирование программой AVG активных объектов (например, приложений, документов…) при открытии, а также при закрытии. Данная функция помогает защитить компьютер от некоторых разновидностей современных вирусов.

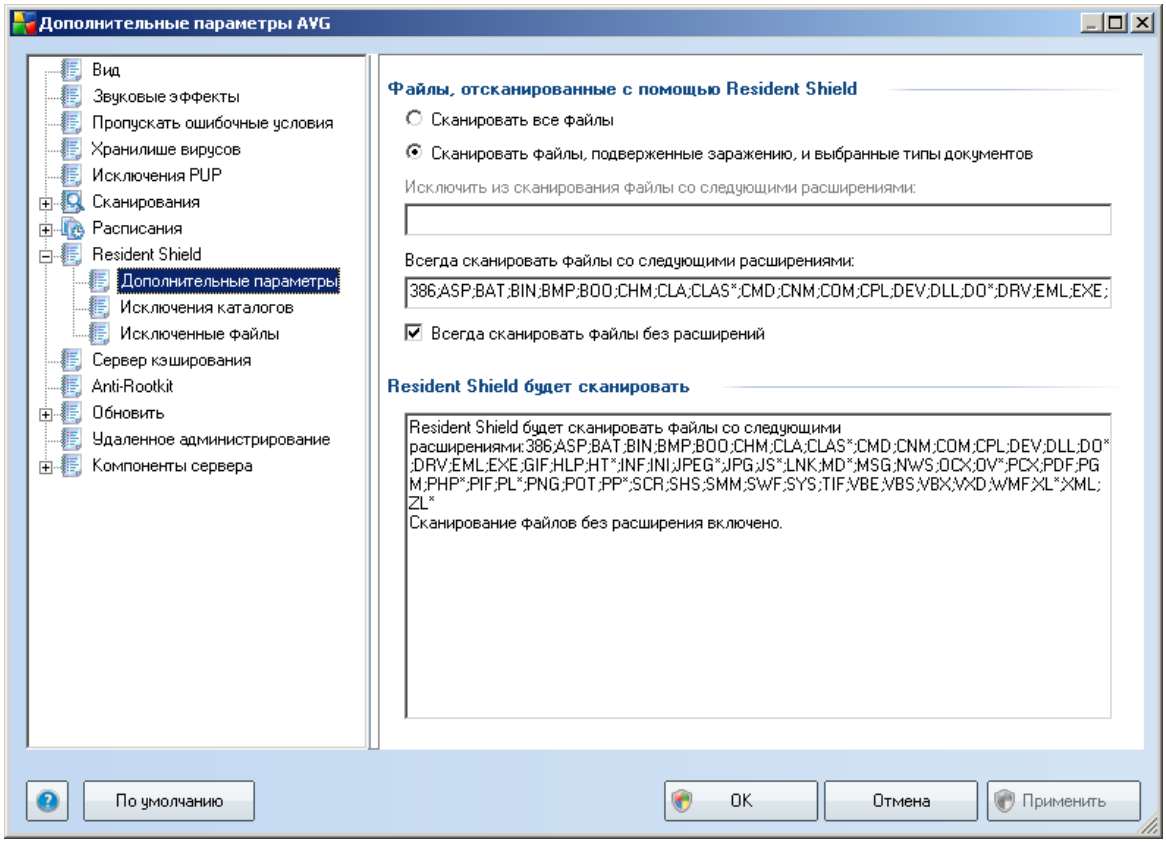
- ***Сканировать загрузочный сектор съемных носителей***. (*По умолчанию включен*).

- ***Использовать эвристический анализ***. (*По умолчанию включен*). Эвристический анализ будет использоваться для обнаружения (*динамическая эмуляция команд сканируемых объектов в виртуальной компьютерной среде*).

- ***Автоматическое лечение***. Любое обнаруженное заражение будет вылечено автоматически, если лечение возможно.

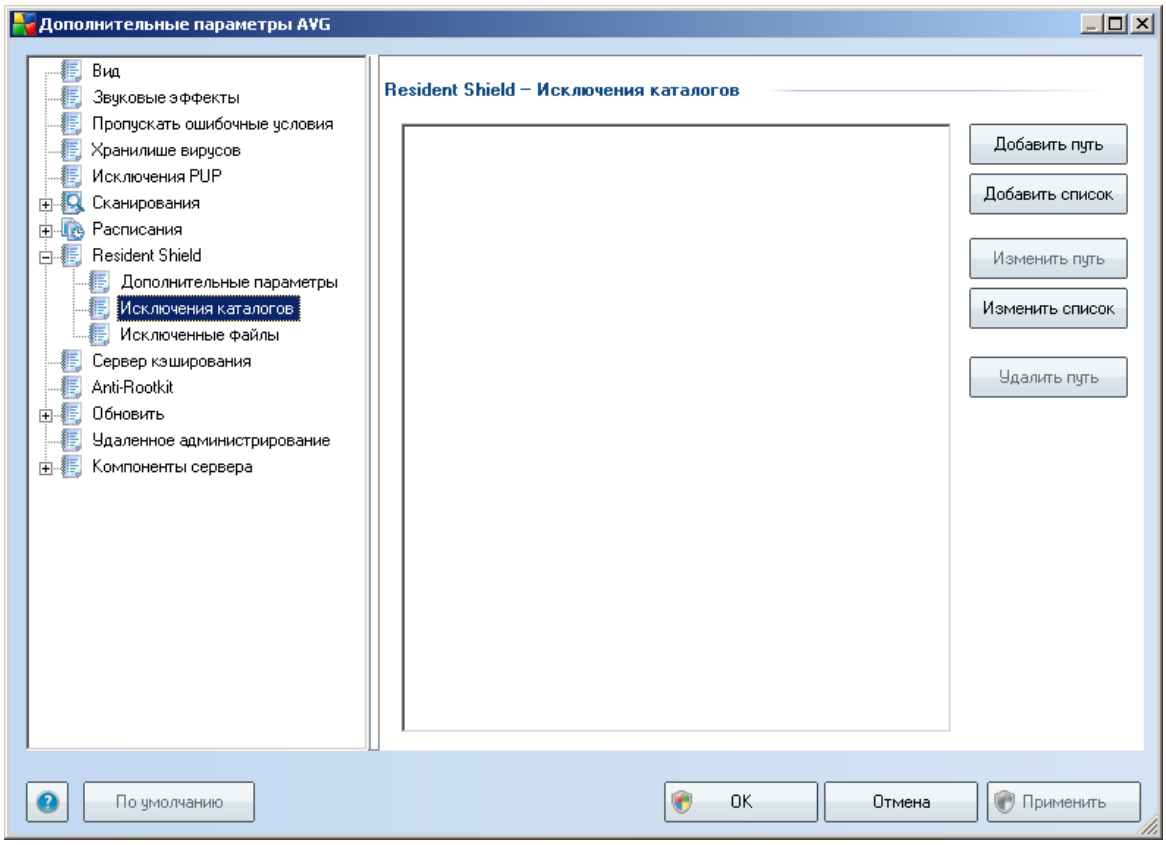
10.8.1. Дополнительные параметры

В диалоговом окне ***Файлы, сканируемые с помощью компонента Resident Shield*** можно указать файлы, которые необходимо сканировать (*по определенным расширениям*):



Определение необходимости сканировать все файлы или только файлы, подверженные заражению. В данном случае далее можно указать список расширений, определяющих файлы, которые сканировать не нужно, а также список расширений файлов, которые необходимо сканировать в любом случае.

10.8.2. Исключаемые каталоги



Диалоговое окно ***Resident Shield — Исключения каталогов*** позволяет определить папки, которые должны быть исключены из сканирования компонентом ***Resident Shield.***

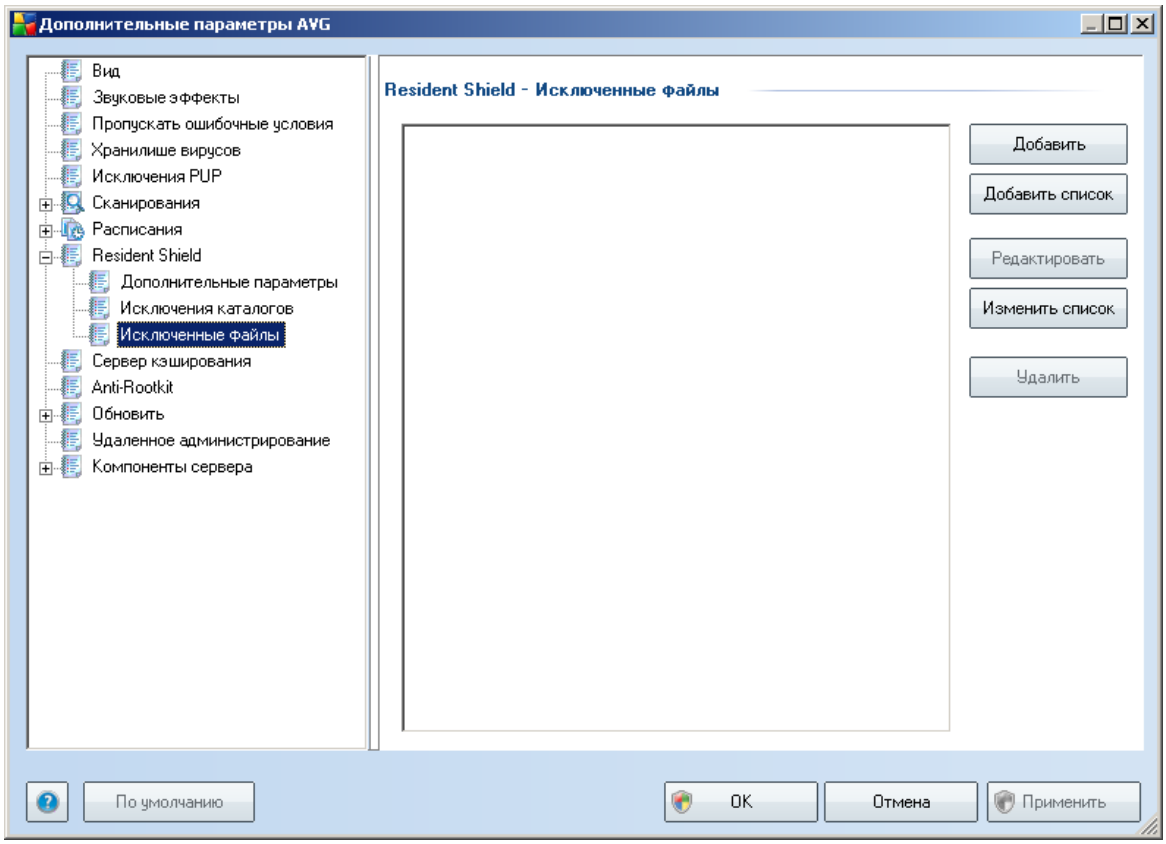
Настоятельно рекомендуется не исключать папки без необходимости.

В диалоговом окне содержатся следующие кнопки управления:

- ***Добавить путь***— укажите каталоги, которые должны быть исключены из сканирования, выбрав их последовательно в навигационном дереве локального диска.
- ***Добавить список***— позволяет ввести полный список каталогов, которые должны быть исключены из сканирования компонентом ***Resident Shield***
- ***Изменить путь***— позволяет изменить указанный путь к выбранной папке.

- ***Редактировать список***— позволяет редактировать список папок
- ***Удалить путь***— позволяет удалить путь к выбранной папке из списка.

10.8.3. Исключенные файлы



Диалоговое окно ***Resident Shield — Исключенные файлы*** работает так же, как ранее описанное ***Resident Shield — Исключения каталогов***, но вместо папок теперь можно указать определенные файлы, которые не должны сканироваться компонентом ***Resident Shield.***

Настоятельно рекомендуется не исключать файлы без необходимости.

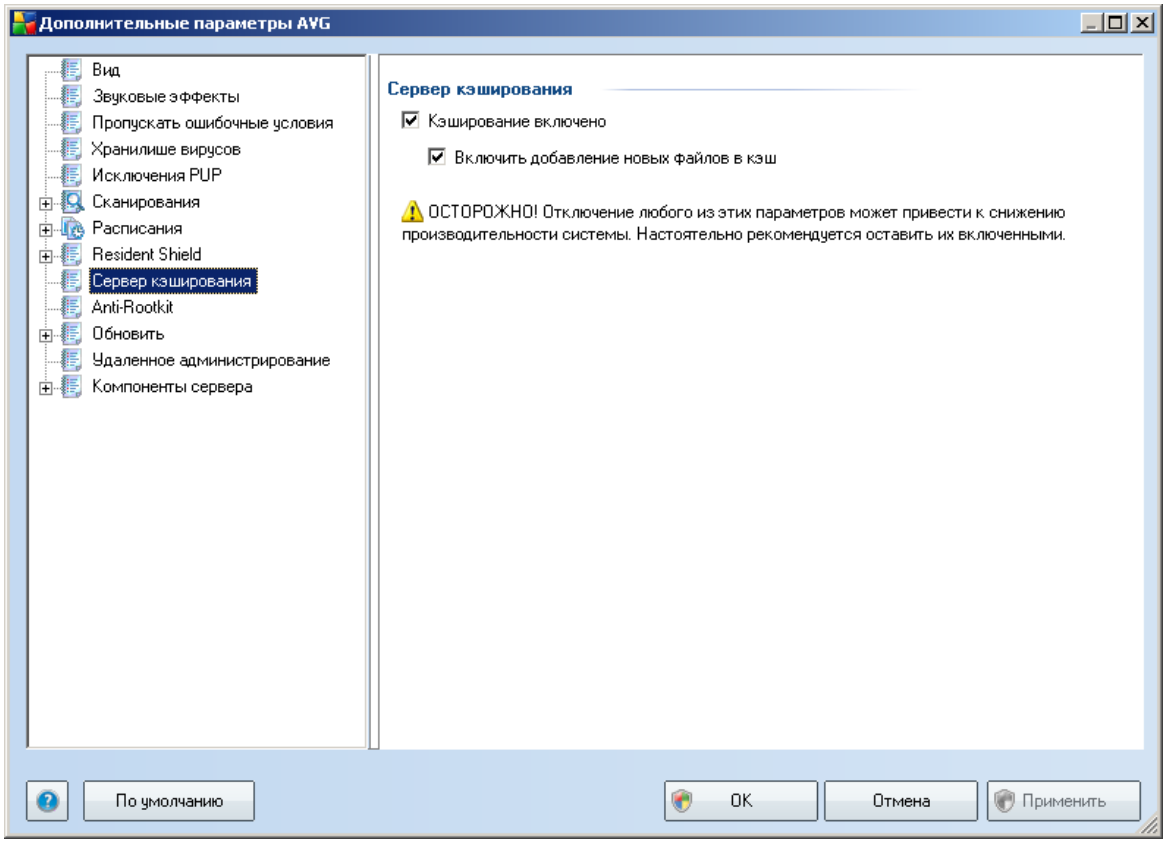
В диалоговом окне содержатся следующие кнопки управления:

- ***Добавить***. Укажите файлы, которые должны быть исключены из сканирования, выбрав их последовательно в навигационном дереве локального диска.

- ***Добавить список***. Позволяет ввести полный список файлов, которые должны быть исключены из сканирования компонентом ***Resident Shield***.
- ***Редактировать***. Позволяет редактировать указанный путь к выбранному файлу.
- ***Редактировать список***. Позволяет редактировать список файлов.
- ***Удалить***. Позволяет удалить путь к выбранному файлу из списка.

10.9. Сервер кэширования

Сервер кэширования — это процесс, позволяющий более быстро выполнять операции сканирования (*сканирование по требованию, запланированное сканирование всего компьютера, сканирование с помощью Resident Shield*). Он собирает и хранит информацию о надежных файлах (*системные файлы с цифровой подписью и т. д.*): затем эти файлы определяются как безопасные и пропускаются во время сканирования.



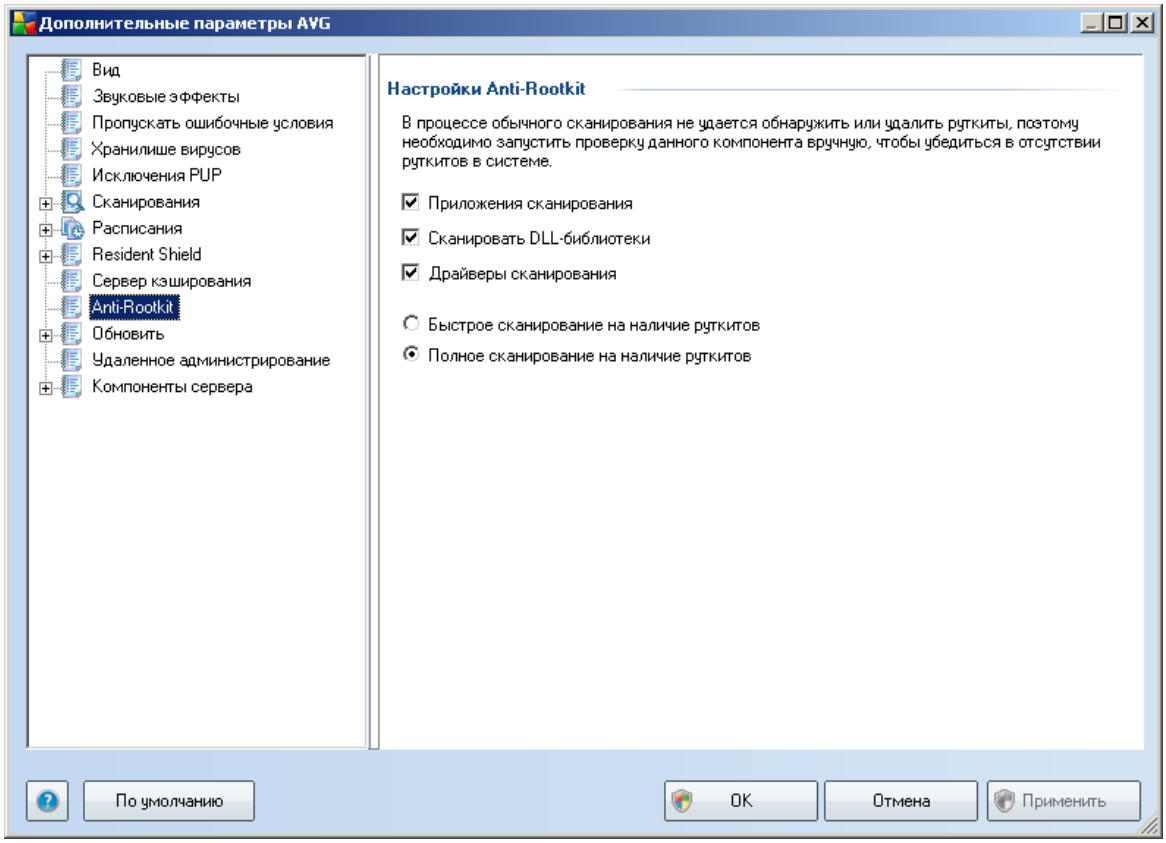
Диалоговое окно настройки содержит два параметра.

- ***Кэширование включено*** (*по умолчанию флажок установлен*). Снимите данный флажок, чтобы выключить ***сервер кэширования*** и очистить кэш-память. Примите к сведению, что сканирование может замедлять работу системы и влиять на общую производительность компьютера, так как каждый используемый файл будет проверяться на предмет вирусов и шпионского ПО.

- ***Включить добавление новых файлов в кэш*** (*по умолчанию флажок установлен*). Снимите данный флажок, чтобы остановить добавление новых файлов в кэш-память. Все добавленные в кэш-память файлы будут храниться и использоваться, пока не будет выключено кэширование или не будет обновлена вирусная база.

10.10. Anti-Rootkit

С помощью данного диалогового окна можно изменить параметры компонента ***Anti-Rootkit***.



Возможность изменения всех функций компонента ***Anti-Rootkit*** , доступная в данном диалоговом окне, также доступна непосредственно в ***интерфейсе компонента Anti-Rootkit***.

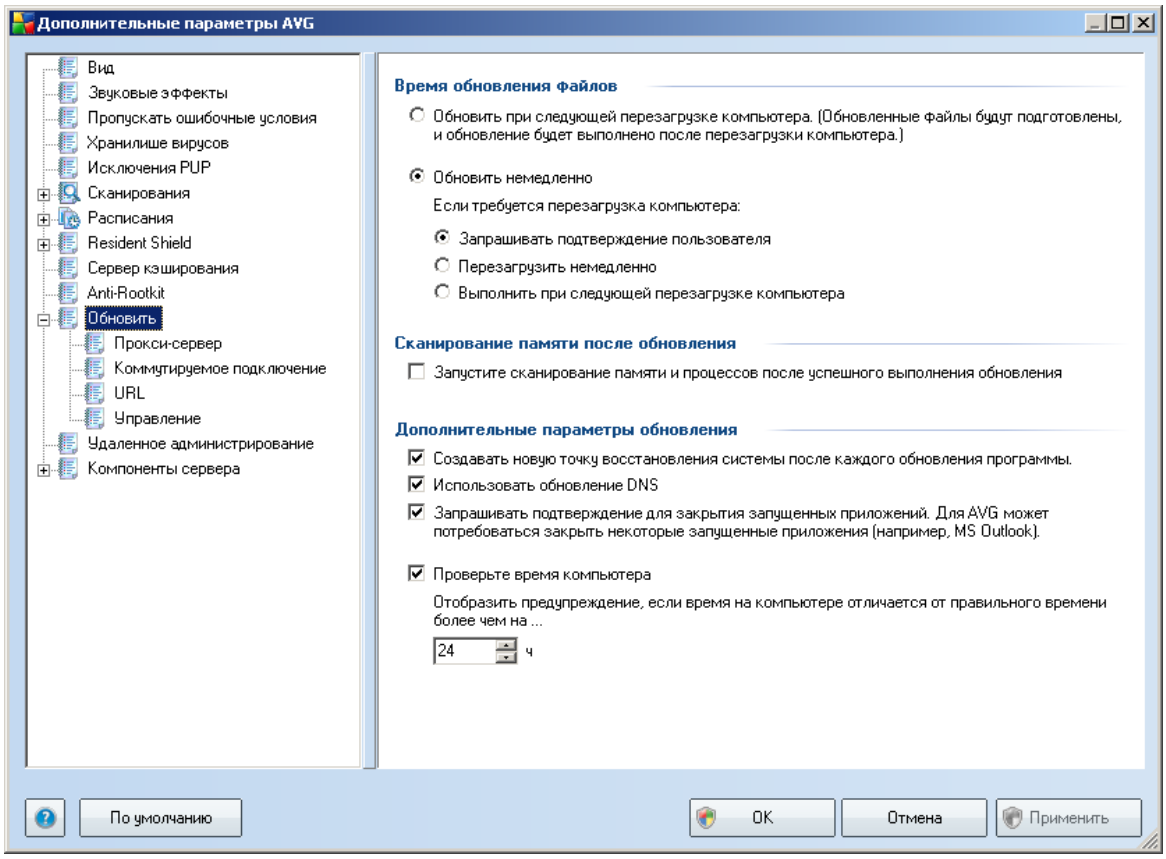
Чтобы указать объекты, которые должны сканироваться, установите соответствующие флажки.

- ***Сканировать приложения***
- ***Сканировать DLL-библиотеки***
- ***Сканировать драйверы***

Далее можно включить режим сканирования на наличие средств rootkit.

- ***Быстрое сканирование rootkit*** — сканирование только системной папки (*обычно c:\Windows*)
- ***Полное сканирование rootkit*** — сканирование всех доступных дисков, за исключением дисков A: и B:.

10.11. Обновление



Элемент навигации ***Обновление*** открывает новое диалоговое окно, в котором можно указать общие параметры обновления продукта AVG.

Время обновления файлов

В этом разделе можно выбрать один из двух вариантов: выполнять обновление при следующей перезагрузке компьютера или выполнять обновление немедленно. Для обеспечения максимального уровня безопасности по умолчанию выбран второй вариант (немедленное обновление). Первый вариант (обновление при следующей перезагрузке компьютера) следует выбирать только в том случае, если вы уверены, что перезагрузка компьютера выполняется не реже одного раза в день.

Если вы решили не изменять конфигурацию по умолчанию и немедленно запускать обновление, можно выбрать условия, при которых будет выполнена перезагрузка компьютера.

- ***Запрашивать подтверждение пользователя***. Появится запрос на подтверждение перезагрузки, необходимой для завершения процесса обновления
- ***Мгновенная перезагрузка***. Перезагрузка будет выполнена автоматически сразу после завершения процесса обновления. Запрос на подтверждение отображаться не будет.
- ***Завершить при следующей перезагрузке*** . Завершение процесса обновления будет отложено до следующей перезагрузки компьютера (обратите внимание, что этот вариант следует выбирать только в том случае, если вы уверены, что перезагрузка компьютера выполняется не реже одного раза в день).

Сканирование памяти после обновления

Установите этот флажок, если требуется запускать сканирование памяти после каждого успешно завершенного обновления. Последнее загруженное обновление может содержать новые определения вирусов, которые сразу должны быть применены при сканировании.

Дополнительные параметры обновления

- ***Создавать новую точку восстановления системы после каждого обновления программы***. Перед каждым запуском обновления программы AVG будет создаваться точка восстановления системы. Если не удастся выполнить обновление или произойдет сбой в работе ОС, всегда можно будет восстановить начальную конфигурацию ОС с этой точки. Данный параметр доступен в меню "Пуск/Все программы/Стандартные/Служебные/Восстановление системы". Однако любые изменения следует вносить только опытным пользователям. Не снимайте этот флажок, если данный

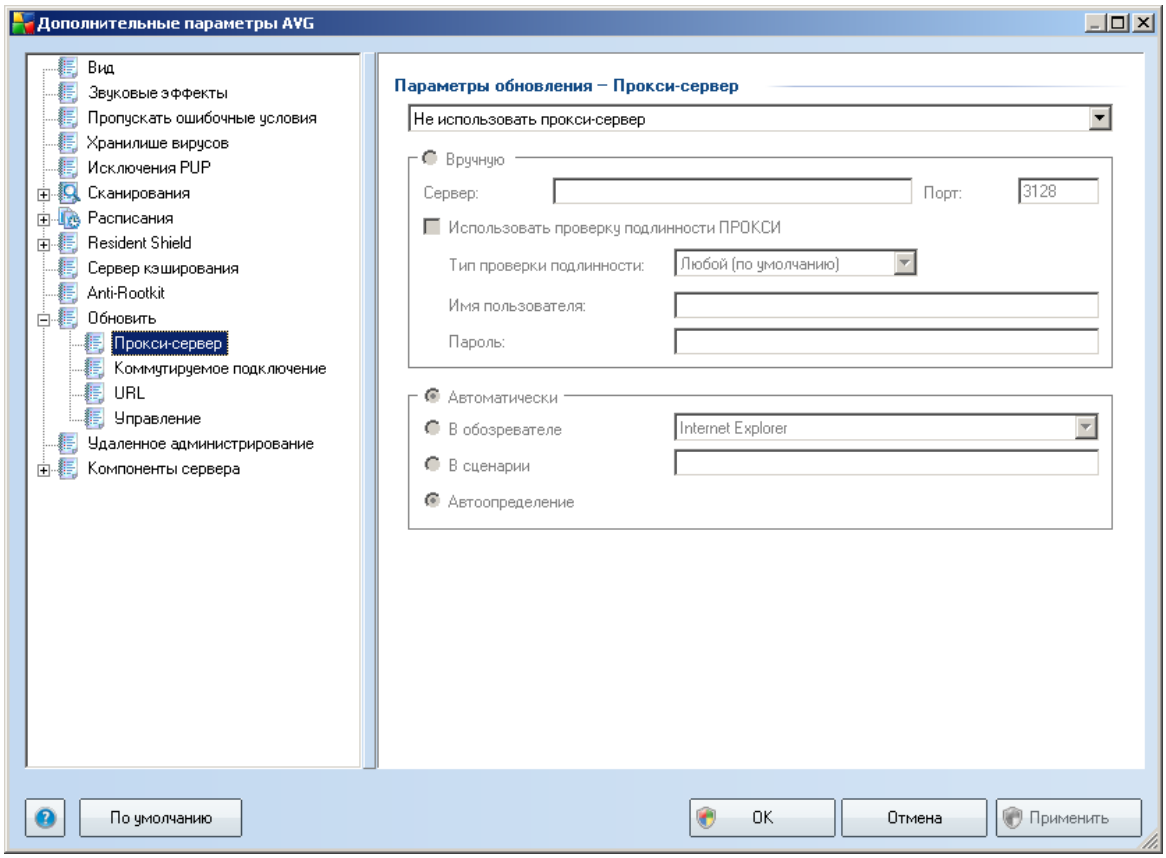
параметр будет использоваться.

- ***Использовать обновление DNS***. Установите этот флажок, чтобы подтвердить необходимость использования способа обнаружения файлов обновлений, что позволит избежать передачи данных между сервером обновлений и клиентом AVG.

- ***Запрашивать подтверждение на закрытие запущенных приложений*** (*используется по умолчанию*). Благодаря этой функции пользователи могут быть уверены, что ни одно из запущенных приложений не будет закрыто без соответствующего разрешения (если это необходимо для завершения процесса обновления).

- ***Проверять время компьютера***. Установите данный флажок для отображения уведомления в случаях, когда время компьютера отличается от правильного на указанное количество часов.

10.11.1. Прокси-сервер



Прокси-сервер — это автономный сервер или служба, запущенная на ПК и гарантирующая безопасное подключение к Интернету. В соответствии с определенными правилами сетей доступ к Интернету можно получить напрямую или через прокси-сервер; оба способа могут использоваться одновременно. В раскрывающемся списке первой части диалогового окна ***Параметры обновления — Прокси-сервер*** выберите необходимые действия.

- ***Использовать прокси-сервер***
- ***Не использовать прокси-сервер***. Параметр по умолчанию.
- ***Подключиться с помощью прокси-сервера, если не удается — подключиться напрямую***

При выборе параметров, использующих прокси-сервер, необходимо указать

некоторые дополнительные данные. Параметры сервера можно настроить автоматически или вручную.

Настройка вручную

При выборе настройки вручную (выберите *параметр **Вручную**, чтобы активировать соответствующий раздел диалогового окна*) необходимо указать следующие данные.

- ***Сервер***. Укажите IP-адрес или имя сервера.
- ***Порт*** — укажите номер порта, через который осуществляется подключение к Интернету (*номер по умолчанию — 3128, но можно задать и другой номер — если вы не уверены в правильности номера порта, обратитесь к системному администратору*)

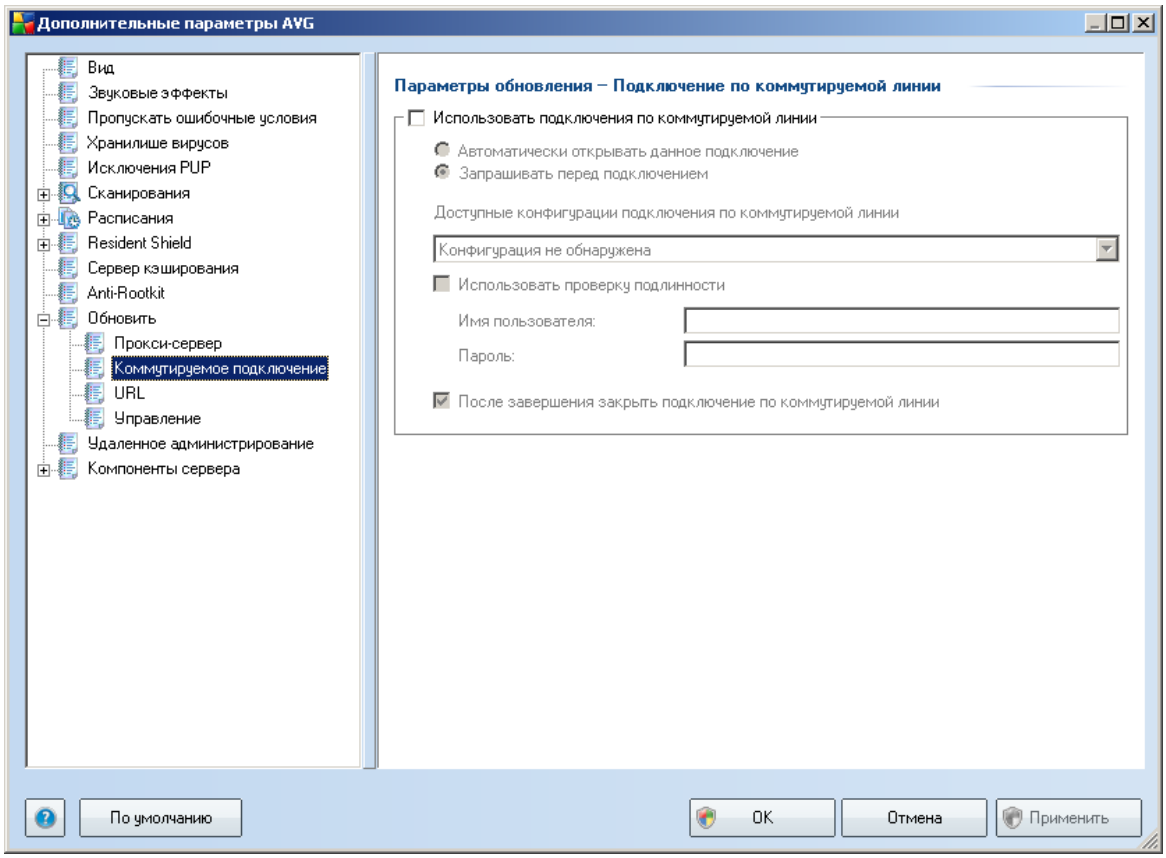
На прокси-сервере также могут быть заданы определенные правила для каждого пользователя. В этом случае установите флажок ***Использовать проверку подлинности ПРОКСИ***, чтобы программа выполняла проверку подлинности имени пользователя и пароля перед подключением к Интернету через прокси-сервер.

Автоматическая настройка

В случае выбора автоматической настройки *(установите флажок **Автоматически**, чтобы активировать соответствующий раздел диалогового окна*), а затем выберите необходимый источник конфигурации прокси-сервера.

- ***Из браузера*** — конфигурация будет считана с интернет-браузера по умолчанию
- ***Из сценария*** — конфигурация будет считана с загруженного сценария с функцией возврата адреса прокси-сервера
- ***Автоопределение*** — конфигурация будет определена автоматически непосредственно на прокси-сервере

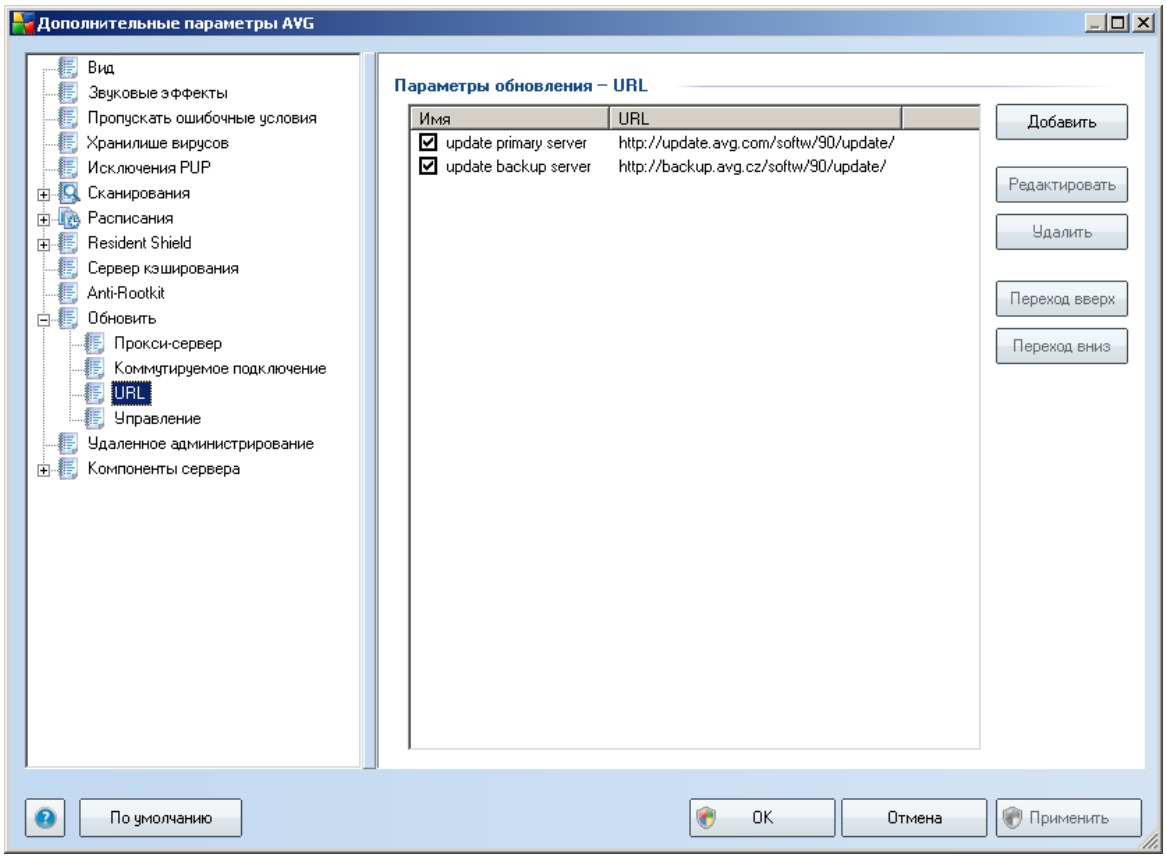
10.11.2. Подключение по коммутируемой линии



Все параметры, дополнительно заданные в диалоговом окне ***Параметры обновления — подключение по коммутируемой линии***, относятся к подключению к Интернету по коммутируемой линии. Чтобы активировать поля диалогового окна, выберите параметр ***Использовать подключения по коммутируемой линии.***

Укажите способ подключения к Интернету: автоматически (***Автоматическое открытие подключения***) или подтверждение каждого подключения вручную (***Спрашивать перед подключением***). Для автоматического подключения также можно определить автоматическое закрытие подключения после обновления (***Автоматически закрыть подключение по коммутируемой линии по завершении***).

10.11.3. URL-адрес



В диалоговом окне ***URL-адрес*** приведен список интернет-адресов, по которым можно загрузить файлы обновлений. Данный список и его элементы можно изменить с помощью следующих кнопок управления.

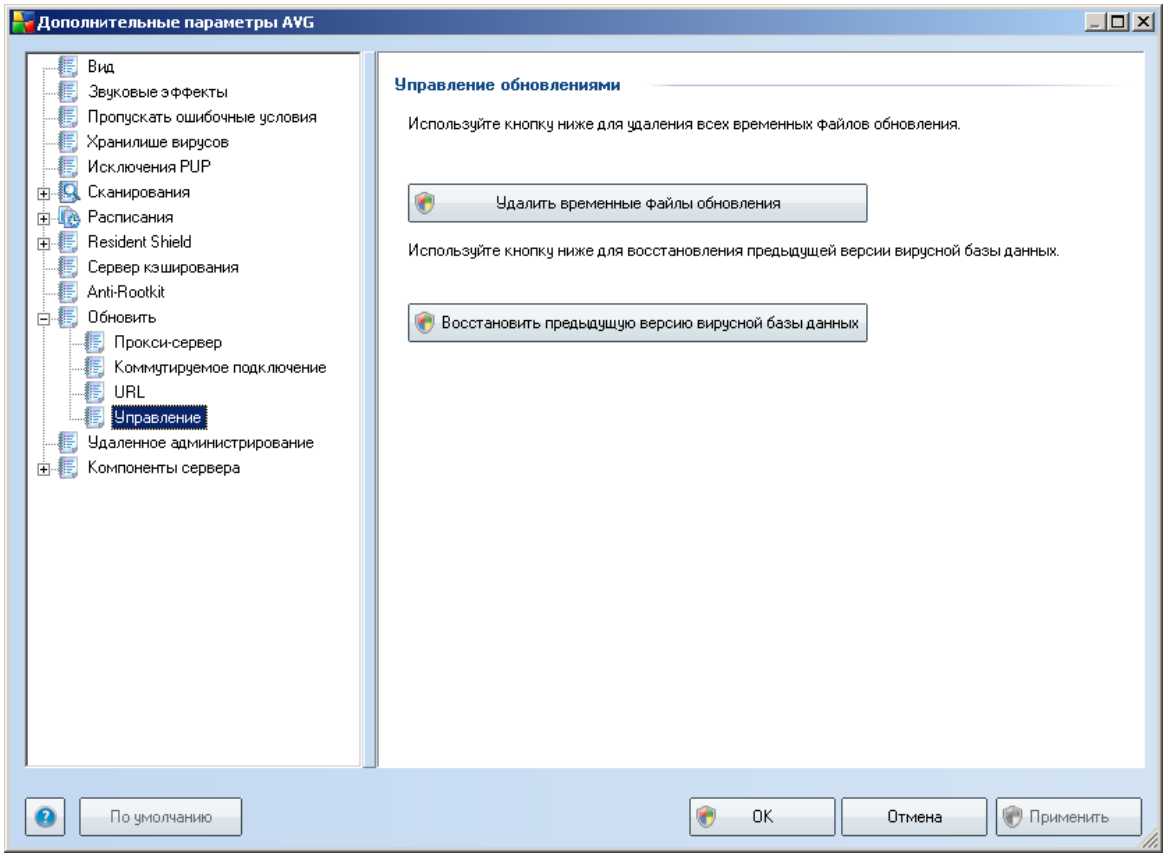
- ***Добавить***. Открывает диалоговое окно, в котором можно указать новый URL-адрес для добавления в список.
- ***Редактировать***. Открывает диалоговое окно, в котором можно изменить параметры выбранного URL-адреса.
- ***Удалить***. Позволяет удалить выбранный URL-адрес из списка.
- ***Переход вверх/Переход вниз***. Эти две кнопки выполняют важную функцию. Первый сервер в списке всегда используется первым при попытке выполнить обновление. Таким образом, перемещение серверов в

списке вверх или вниз обеспечивает изменение их приоритета. При нажатии кнопки ***Переход вверх*** выбранный URL-адрес перемещается в списке на одну позицию вверх, а при нажатии кнопки ***Переход вниз*** — на одну позицию вниз.

При снятии флажка рядом с именем сервера соответствующий сервер будет временно отключен (и его не требуется удалять из списка).

10.11.4. Управление

В диалоговом окне ***Управление*** доступны два параметра, доступ к которым можно получить с помощью двух кнопок.

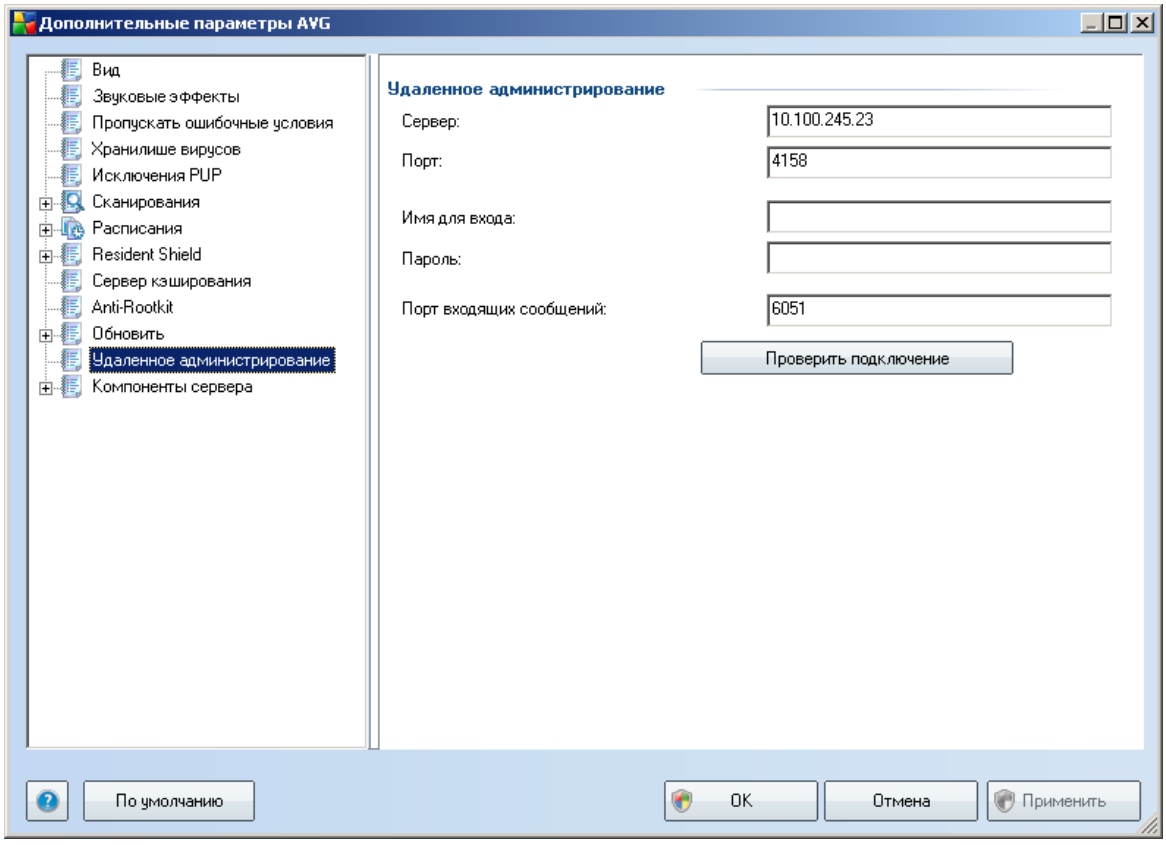


- ***Удалить временные файлы обновлений*** . Нажмите данную кнопку, чтобы удалить все резервные файлы обновлений с жесткого диска (*по умолчанию эти файлы сохраняются в течение 30 дней*)

- ***Восстановить предыдущую версию вирусной базы данных*** — нажмите эту кнопку, чтобы удалить последнюю версию вирусной базы данных с компьютера и восстановить версию, сохраненную ранее (*новая версия базы данных будет входить в следующий пакет обновления*)

10.12. Удаленное администрирование

Элемент ***Удаленное администрирование*** отображается в области ***Дополнительные параметры*** только в том случае, если ранее была выбрана установка компонента ***Удаленное администрирование***, т. е. во время процесса установки был установлен соответствующий флажок в диалоговом окне ***Выбор компонентов***.



Параметры элемента ***Удаленное администрирование*** предназначены для настройки подключения клиентской рабочей станции AVG к системе удаленного администрирования. Для подключения соответствующей станции к системе удаленного администрирования необходимо указать следующие параметры.

- ***Сервер***. Имя сервера (или IP-адрес сервера), на котором установлен сервер администратора AVG.
- ***Порт***. Номер порта, с помощью которого клиент AVG устанавливает соединение с сервером администратора AVG (*номер порта 4158 установлен по умолчанию; если используется данный номер порта, нет необходимости его указывать*).
- ***Имя пользователя***. Если используется безопасное соединение между клиентом AVG и сервером администратора AVG, необходимо указать имя пользователя.
- ***Пароль***. Также необходимо указать пароль.
- ***Порт входящих сообщений***. Номер порта, через который клиент AVG принимает входящие сообщения от сервера администратора AVG.

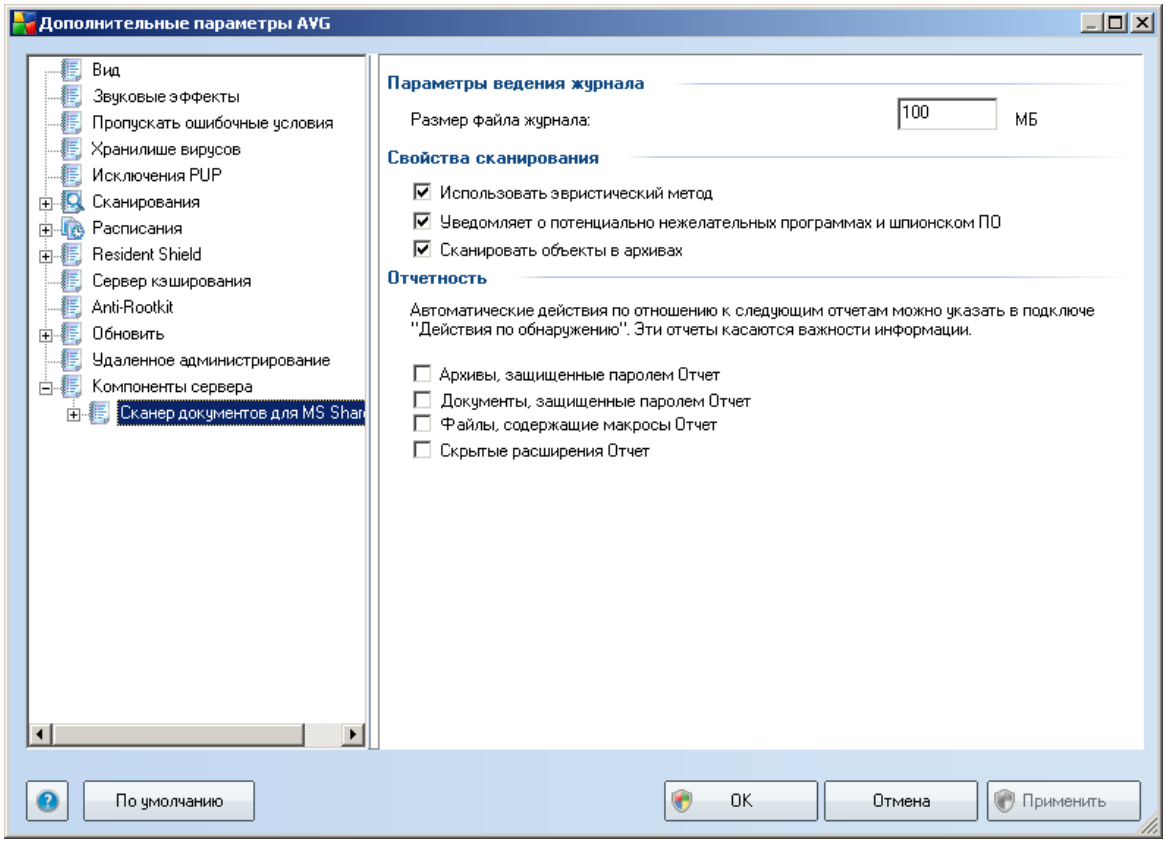
Кнопка ***Проверить подключение*** позволяет удостовериться, что вся упомянутая выше информация является допустимой и может быть использована для успешного соединения с DataCenter.

Примечание. *Подробное описание системы удаленного администрирования см. в документации, прилагаемой к AVG Business Edition.*

10.13. Компоненты сервера

10.13.1. Document Scanner для MS SharePoint

В данном диалоговом окне будет отображено несколько предварительно настроенных параметров, связанных с производительностью сканирования документов на наличие вирусов компонентом ***Document Scanner для MS SharePoint***. Диалоговое окно разделено на несколько разделов.



Параметры ведения журнала

Поле **Размер файла журнала**. Файл журнала содержит записи о различных событиях компонента ***Document Scanner для MS SharePoint***, например уведомления о загрузке программных библиотек, события обнаружения вирусов, предупреждения об устранении неполадок и т. д. Максимальный размер файла журнала можно установить в текстовом поле.

Свойства сканирования

- ***Использовать эвристический анализ***. Установите флажок, чтобы использовать эвристический метод обнаружения при сканировании документов. Включение данного параметра позволяет выполнить фильтрацию документов не только по их расширению, но также с учетом фактического содержимого документов.

- ***Уведомлять о потенциально нежелательных программах и угрозах появления шпионского ПО***. Установите флажок, чтобы использовать модуль Anti-Spyware, например для обнаружения и создания отчетов о подозрительных и потенциально нежелательных программах при сканировании документов.

- ***Сканировать объекты в архивах***. Установите данный флажок, чтобы сканировать содержимое архивов.

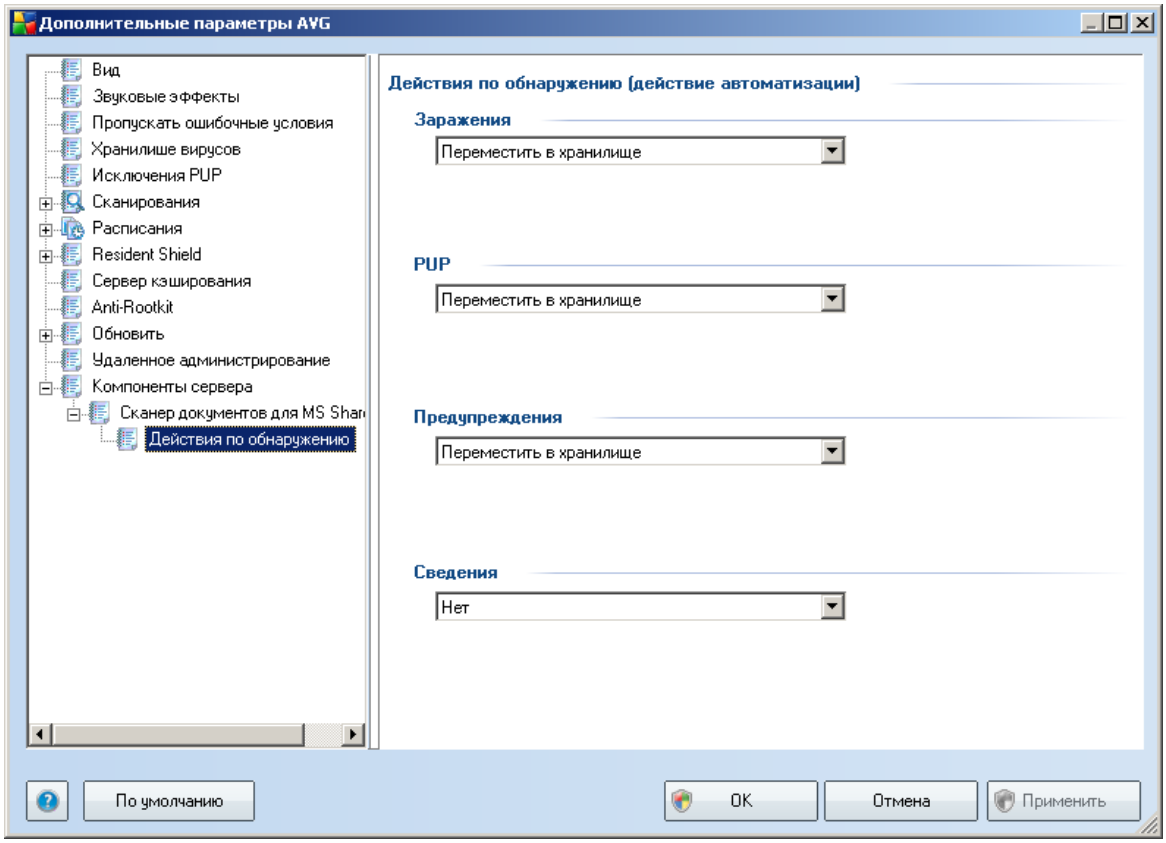
Отчетность

- ***Сообщать об архивах, защищенных паролем***. Сканирование на наличие вирусов в архивах (ZIP, RAR и т. п.), защищенных паролем, недоступно; установите флажок, чтобы в отчетах они были отмечены как потенциально опасные.

- ***Сообщать о документах, защищенных паролем***. Сканирование на наличие вирусов в документах, защищенных паролем, недоступно; установите флажок, чтобы в отчетах они были отмечены как потенциально опасные.

- ***Сообщать о файлах, содержащих макросы***. Макрос — предустановленная последовательность действий, предназначенная для упрощения выполнения пользователем определенных задач (широко известны макросы MS Word). По этой причине макросы могут содержать потенциально опасные инструкции и пользователю, возможно, потребуется установить флажок, чтобы файлы с макросами были отмечены в отчетах как подозрительные.

- ***Сообщать о скрытых расширениях***. Скрытое расширение может способствовать отображению, например, подозрительного исполняемого файла something.txt.exe как безопасного обычного текстового файла something.txt; установите флажок, чтобы в отчетах данные файлы были отмечены как потенциально опасные.



В этом диалоговом окне можно настроить поведение компонента ***Document Scanner для MS SharePoint*** при обнаружении угроз. Угрозы поделены на следующие категории.

- ***Заражения***. Вредоносные коды, способные копировать себя и самостоятельно распространяться; часто остаются незамеченными, пока не нанесут вред.
- ***Потенциально нежелательные программы (PUP)***. Такие программы отличаются от обычных программ тем, что представляют угрозу персональным данным пользователя.
- ***Предупреждения***. Обнаруженные объекты, сканирование которых не удалось выполнить.
- ***Информация***. Обнаруженные потенциальные угрозы, которые не удалось

классифицировать по вышеуказанным категориям.

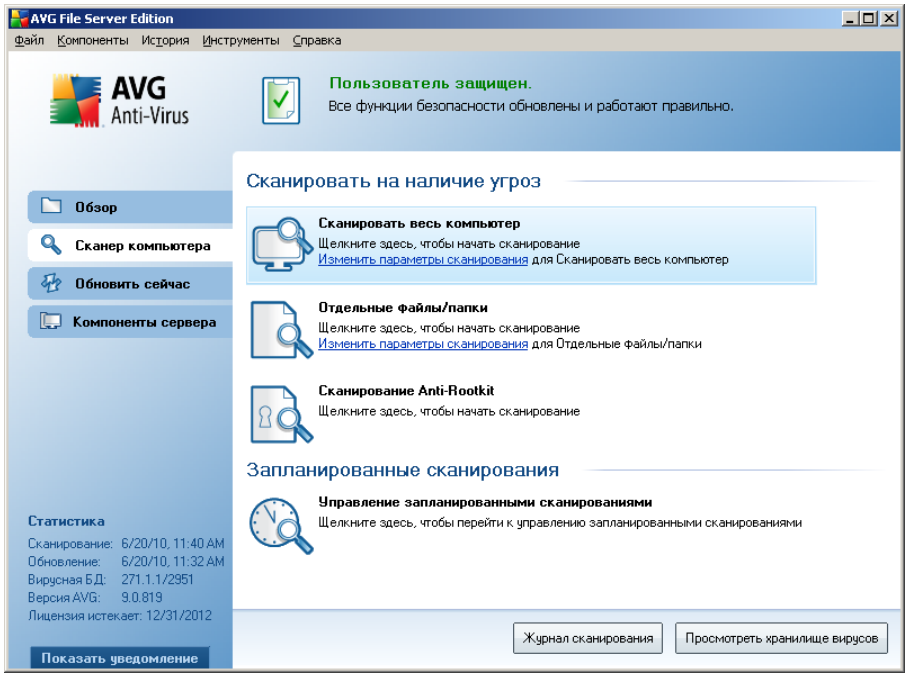
С помощью раскрывающихся меню выберите автоматические действия для перечисленных угроз.

- ***Нет***. С документами, содержащими такие угрозы, не будут выполняться никакие действия.
- ***Переместить в хранилище***. Каждый зараженный документ будет перемещен в зону карантина хранилища вирусов.
- ***Удалить***. Документ с обнаруженным вирусом будет удален.

11. Сканирование AVG

Сканирование — это одна из важнейших функций **AVG 9.0 File Server**. Можно выполнять проверки по требованию или планировать их периодический запуск в удобное для вас время.

11.1. Интерфейс сканирования



Для перехода к интерфейсу сканирования AVG необходимо выбрать быструю ссылку ***Сканер компьютера***. Щелкните эту ссылку, чтобы открыть диалоговое окно ***Сканирование на наличие угроз***. Данное диалоговое окно содержит следующие разделы:

- обзор предопределенных сканирований — три типа сканирований, определенных поставщиком ПО, готовые к использованию по расписанию или при необходимости:
    - ***Сканирование всего компьютера***
    - ***Сканировать отдельные файлы или папки***
    - ***Сканирование Anti-Rootkit***

- Раздел "Расписание сканирования" — в данном разделе можно настроить новые проверки и создать новые расписания при необходимости.

Кнопки управления

В интерфейсе проверки доступны следующие кнопки управления:

- ***Журнал сканирования*** — открывает диалоговое окно Обзор результатов сканирования, содержащее полную историю сканирования
- ***Просмотреть хранилище вирусов*** — открывает новое окно Хранилище вирусов — место хранения обнаруженных вирусов

11.2. Предопределенные сканирования

Одна из главных функций **AVG 9.0 File Server** — сканирование по требованию. Проверка по требованию разработана для сканирования различных частей компьютера при подозрении на заражение вирусом. Рекомендуется проводить такие проверки регулярно, даже в случае видимого отсутствия вируса на компьютере.

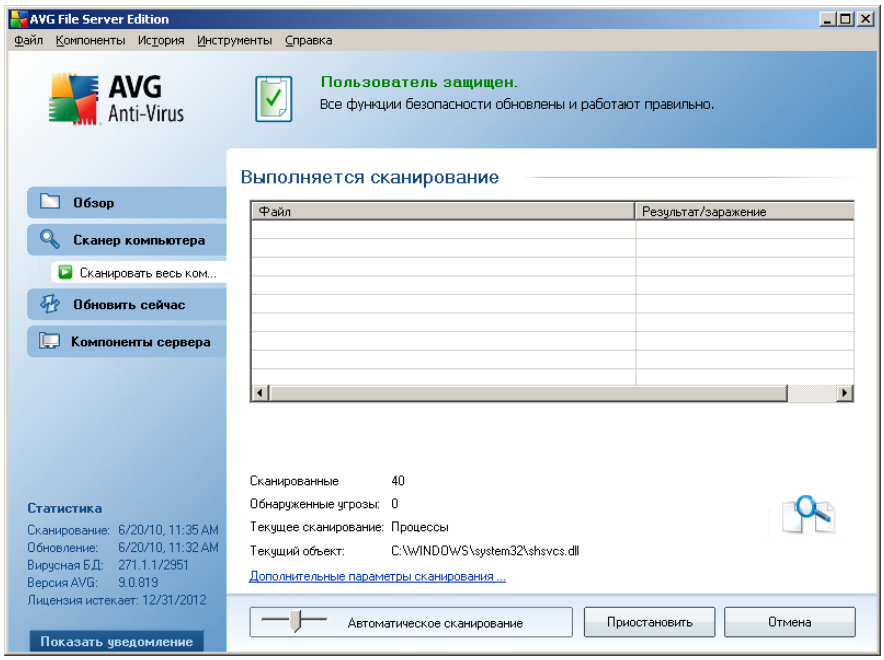
В системе **AVG 9.0 File Server** доступны следующие типы сканирования, настроенные поставщиком программного обеспечения.

11.2.1. Сканирование всего компьютера

Сканировать весь компьютер — сканирование всего компьютера на наличие заражений и/или потенциально нежелательных программ. При данном типе проверки выполняется сканирование всех жестких дисков компьютера, производится обнаружение и лечение зараженных объектов или перемещение в ***хранилище вирусов***. Сканирование всего компьютера необходимо выполнять на рабочих станциях как минимум один раз в неделю.

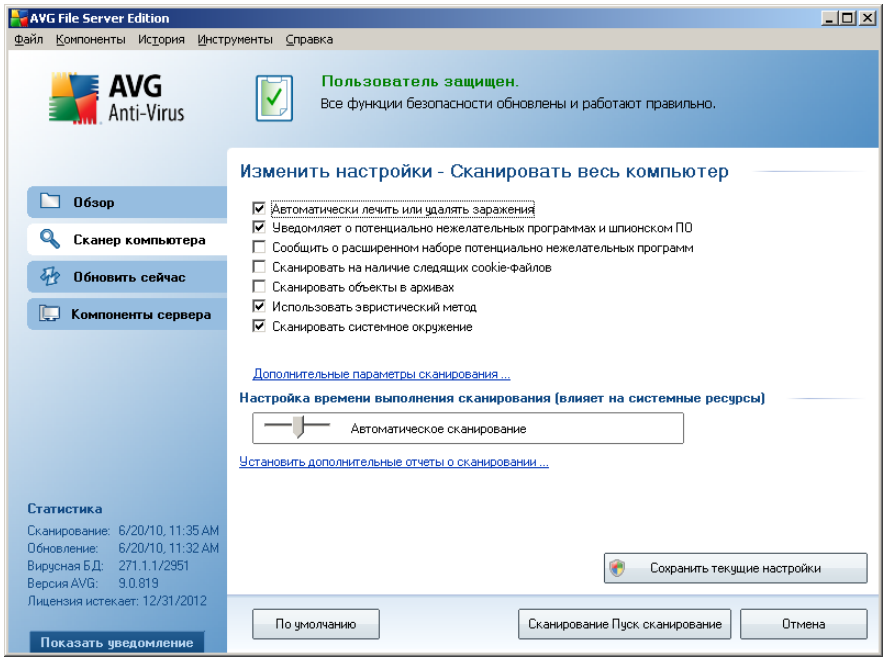
Запуск сканирования

Сканирование всего компьютера можно запустить непосредственно в интерфейсе сканирования, щелкнув значок сканирования. При данном типе сканирования не требуются какие-либо дополнительные настройки, процесс сканирования начнется немедленно при открытии диалогового окна ***Выполняется сканирование*** (*см. снимок экрана*). При необходимости сканирование можно прервать (***Пауза***) или отменить (***Отмена***).



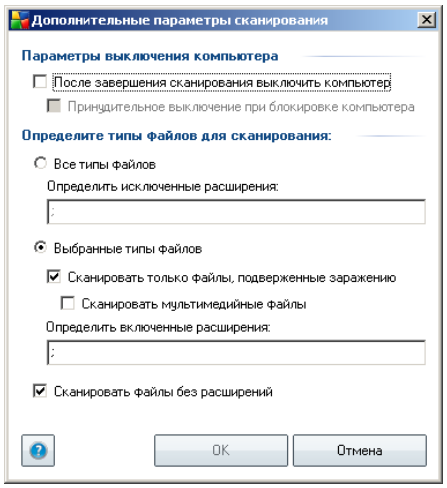
Изменение параметров сканирования

Существует возможность изменения предварительно определенных параметров ***сканирования всего компьютера***. Щелкните ссылку ***Изменить параметры сканирования***, чтобы открыть диалоговое окно ***Изменение параметров сканирования всего компьютера. Рекомендуется сохранять установленные по умолчанию настройки до появления веской причины для их изменения!***



- ***Параметры сканирования***. В списке параметров сканирования можно включить или выключить определенные параметры при необходимости. По умолчанию большинство параметров включены и используются автоматически при сканировании.

- ***Дополнительные параметры сканирования***. Эта ссылка открывает новое диалоговое окно ***Дополнительные параметры сканирования***, где можно указывать следующие параметры.



- ***Параметры выключения компьютера***. Определяет, необходимо ли автоматическое выключение компьютера после завершения процесса сканирования. После выбора этого параметра (***Выключить компьютер после завершения сканирования***) становится доступен новый параметр, позволяющий выключать компьютер, даже если он заблокирован (***Принудительное выключение при блокировке компьютера***).

- ***Определение типов файлов для сканирования***. Далее необходимо указать типы файлов для сканирования.

  - ***Все типы файлов*** с возможностью определения исключений из сканирования посредством предоставления списка расширений файлов, разделенных запятыми, сканирование которых проводиться не будет.

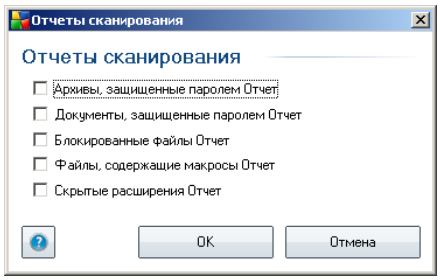
  - ***Выбранные типы файлов***. Можно указать сканирование только тех файлов, которые подвержены заражению (*файлы, не подверженные заражению, не будут сканироваться, например простые текстовые файлы или другие неисполняемые файлы*), включая мультимедийные файлы (*видео- и аудиофайлы — если не устанавливать этот флажок, время сканирования значительно уменьшится, так как эти файлы обладают довольно большим размером и вероятность их заражения вирусом мала*). С помощью расширений можно указать файлы, которые необходимо сканировать всегда.

  - Дополнительно можно установить флажок ***Сканировать файлы без расширений***. Он установлен по умолчанию. Рекомендуется

не изменять его без веских причин. Файлы без расширения являются подозрительными, поэтому необходимо выполнять их сканирование каждый раз.

- ***Приоритет процесса сканирования***. Для изменения приоритета процесса сканирования используйте ползунок. По умолчанию установлен средний уровень приоритета (*Автоматическое сканирование*), который обеспечивает оптимальную скорость процессора и использование системных ресурсов. Также можно запустить процесс сканирования на медленной скорости, чтобы снизить нагрузку на системные ресурсы (*рекомендуется, если пользователю не важно, как долго выполняется сканирование*), или на быстрой с большим потреблением системных ресурсов (*например, если компьютер временно не используется*).

- ***Настроить дополнительные отчеты сканирования***. При нажатии этой ссылки открывается диалоговое окно ***Отчеты сканирования***, в котором можно выбрать типы объектов, сведения о которых должны отображаться в отчете.



Предупреждение. *Перечисленные параметры сканирования действительны также для вновь создаваемого сканирования, как описано в разделе* ***Сканирование AVG/Планирование сканирования/Способы сканирования****. Если потребуется изменить конфигурацию по умолчанию параметра* ***Сканирование всего компьютера****, можно затем сохранить новые параметры в качестве конфигурации по умолчанию, чтобы они использовалась каждый раз при сканировании всего компьютера.*

11.2.2. Сканирование отдельных файлов или папок

Сканирование отдельных файлов или папок — при данном типе сканирования проверяются только области компьютера, выбранные для сканирования (*выбранные папки, жесткие диски, гибкие диски, компакт-диски и т. п.*). Процессы обнаружения вирусов и лечения зараженных объектов при данном типе сканирования будут выполняться также, как и при сканировании всего компьютера: найденные вирусы подвергаются лечению или удаляются в

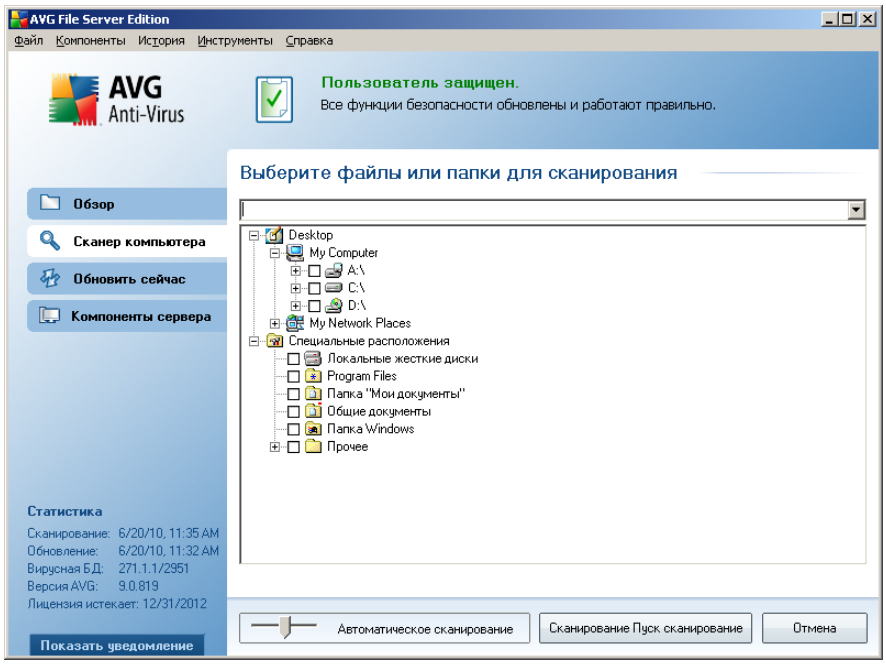
хранилище вирусов. Сканирование отдельных файлов и папок можно использовать при создании пользовательских проверок и их расписаний.

Запуск сканирования

Сканирование отдельных файлов или папок можно запустить непосредственно в интерфейсе сканирования, щелкнув значок сканирования. Откроется новое диалоговое окно ***Выбор отдельных файлов или папок для сканирования***. В древовидной структуре компьютера выберите папки для сканирования. Путь к каждый выбранной папке будет создан автоматически и отобразится в текстовом поле в верхней части данного диалогового окна.

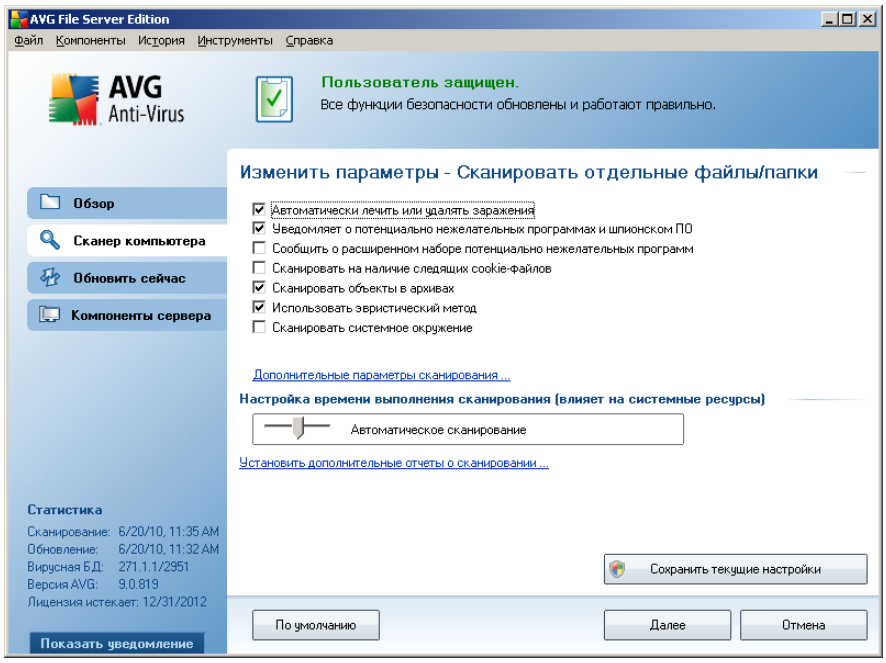
Существует также возможность сканирования определенных папок без сканирования соответствующих подпапок. Чтобы выполнить такое сканирование, введите значок минус "**-**" перед автоматически созданным путем. Чтобы исключить всю папку из процесса сканирования, используйте параметр "!".

Наконец, чтобы запустить сканирование, нажмите кнопку ***Начать сканирование***; данный процесс сканирования практически идентичен процессу сканирования всего компьютера.



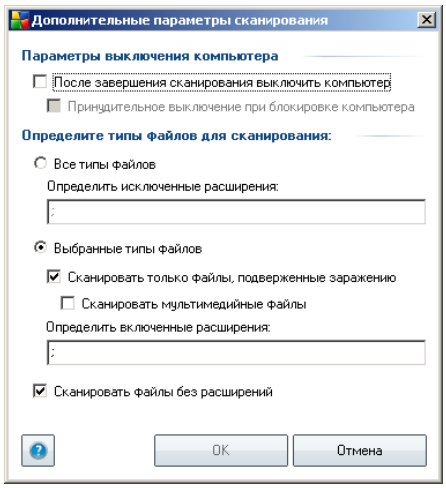
Изменение параметров сканирования

Существует возможность изменения предварительно определенных параметров ***сканирования отдельных файлов и папок***. Щелкните ссылку ***Изменить параметры сканирования***, чтобы открыть диалоговое окно ***Изменение параметров сканирования для сканирования отдельных файлов и папок***. ***Рекомендуется сохранять установленные по умолчанию настройки до появления веской причины для их изменения!***



- ***Параметры сканирования***. В списке параметров сканирования можно включить или отключить определенные параметры при необходимости *(подробное описание данных параметров см. в разделе Расширенные настройки AVG/Сканирования/Сканирование отдельных файлов и папок)*.

- ***Дополнительные параметры сканирования***. Эта ссылка открывает новое диалоговое окно Дополнительные параметры сканирования, где можно указывать следующие параметры.



- ***Параметры выключения компьютера***. Определяет, необходимо ли автоматическое выключение компьютера после завершения процесса сканирования. После выбора этого параметра (***Выключить компьютер по завершении сканирования***) становится доступен новый параметр, позволяющий выключать компьютер, даже если он заблокирован (***Принудительное выключение при блокировке компьютера***).

- ***Определение типов файлов для сканирования***. Далее необходимо определить типы файлов для сканирования.

  - ***Все типы файлов*** с возможностью определения исключений из сканирования посредством предоставления списка расширений файлов, разделенных запятыми, сканирование которых проводиться не будет.

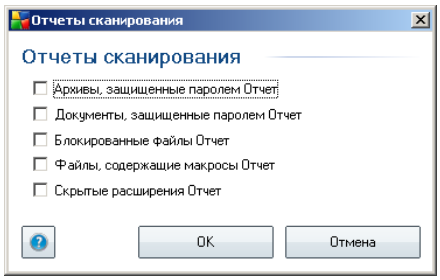
  - ***Выбранные типы файлов***. Можно указать сканирование только тех файлов, которые подвержены заражению (*файлы, не подверженные заражению, не будут сканироваться, например простые текстовые файлы или другие неисполняемые файлы*), включая мультимедийные файлы (*видео- и аудиофайлы — если не устанавливать этот флажок, время сканирования значительно уменьшится, так как эти файлы обладают довольно большим размером и вероятность их заражения вирусом мала*). С помощью расширений можно указать файлы, которые необходимо сканировать всегда.

  - Дополнительно можно установить флажок ***Сканировать файлы без расширений***. Он установлен по умолчанию. Рекомендуется

не изменять его без веских причин. Файлы без расширения являются подозрительными, поэтому необходимо выполнять их сканирование каждый раз.

- ***Приоритет процесса сканирования***. Для изменения приоритета процесса сканирования используйте ползунок. По умолчанию установлен средний уровень приоритета (*Автоматическое сканирование*), который обеспечивает оптимальную скорость процессора и использование системных ресурсов. Также можно запустить процесс сканирования на медленной скорости, чтобы снизить нагрузку на системные ресурсы (*рекомендуется, если пользователю не важно, как долго выполняется сканирование*), или на быстрой с большим потреблением системных ресурсов (*например, если компьютер временно не используется*).

- ***Настроить дополнительные отчеты сканирования***. При нажатии этой ссылки открывается диалоговое окно ***Отчеты сканирования***, в котором можно выбрать типы объектов, сведения о которых должны отображаться в отчете.



Предупреждение. *Перечисленные параметры сканирования действительны также для вновь создаваемого сканирования, как описано в разделе* ***Сканирование AVG/Планирование сканирования/Способы сканирования****. Если потребуется изменить конфигурацию по умолчанию параметра* ***Сканирование отдельных файлов и папок****, можно сохранить новые параметры как конфигурацию по умолчанию, чтобы она использовалась каждый раз при сканировании отдельных файлов или папок. Кроме того, созданная конфигурация может затем использоваться в качестве шаблона для новых запланированных сканирований (все пользовательские сканирования основаны на текущей конфигурации сканирования выбранных файлов и папок).*

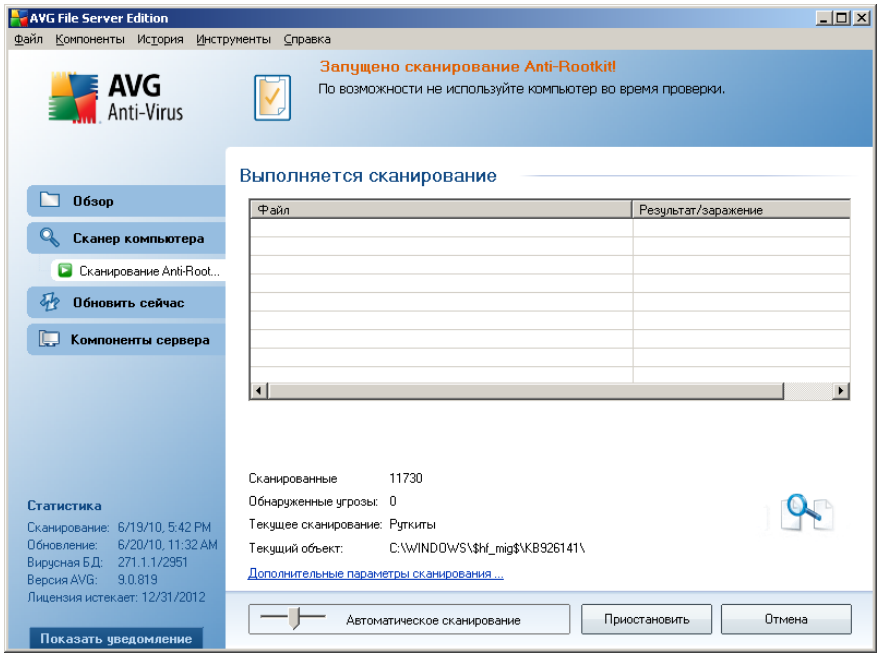
11.2.3. Сканирование Anti-Rootkit

Сканирование Anti-Rootkit исследует компьютер на возможные средства rootkit (*программы и технологии, позволяющие скрыть вредоносную активность на компьютере*). Если программа rootkit обнаружена, это еще не значит, что

компьютер заражен. В некоторых случаях определенные драйверы или разделы обычных приложений могут быть ошибочно приняты за средства rootkit.

Запуск сканирования

Сканирование Anti-Rootkit можно запустить непосредственно из интерфейса сканирования, щелкнув значок сканирования. При данном типе сканирования не требуются какие-либо дополнительные настройки, процесс сканирования начнется немедленно при открытии диалогового окна ***Выполняется сканирование*** (*см. снимок экрана*). При необходимости сканирование можно прервать (***Пауза***) или отменить (***Отмена***).



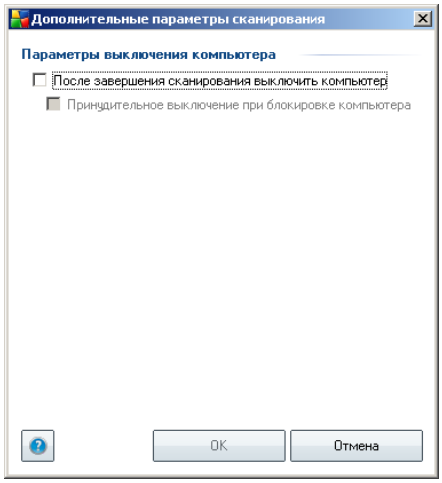
Изменение параметров сканирования

Сканирование Anti-Rootkit всегда запускается по умолчанию, изменение параметров сканирования возможно только в диалоговом окне ***Расширенные настройки AVG/Anti-Rootkit***. В интерфейсе сканирования доступны только следующие настройки.

- ***Автоматическое сканирование***. Для изменения приоритета процесса сканирования используйте ползунок. По умолчанию установлен средний уровень

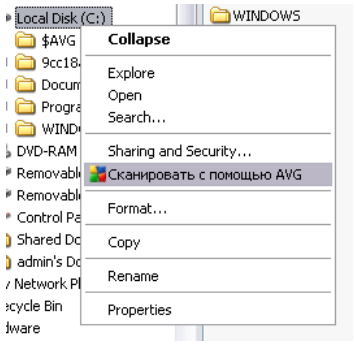
приоритета (*Автоматическое сканирование*), который обеспечивает оптимальную скорость процессора и использование системных ресурсов. Также можно запустить процесс сканирования на медленной скорости, чтобы снизить нагрузку на системные ресурсы (*рекомендуется, если пользователю не важно, как долго выполняется сканирование*), или на быстрой с большим потреблением системных ресурсов (*например, если компьютер временно не используется*).

- ***Дополнительные параметры сканирования***. Данная ссылка открывает новое диалоговое окно ***Дополнительные параметры сканирования***, в котором можно выбрать возможные условия выключения компьютера, связанные со ***сканированием компонентом Anti-Rootkit*** (***Выключить компьютер по завершении сканирования***, *также возможно* ***Принудительное выключение при блокировке компьютера***):



11.3. Сканирование в Проводнике Windows

Кроме предопределенных сканирований всего компьютера или выбранных областей, программа **AVG 9.0 File Server** также имеет функцию быстрого сканирования выбранного объекта непосредственно в Проводнике Windows. Если необходимо открыть неизвестный файл, содержимое которого не вызывает доверия, можно проверить такой файл по запросу. Выполните следующие действия.



- В Проводнике Windows выделите файл (или папку), который необходимо проверить
- Откройте контекстное меню, щелкнув объект правой кнопкой мыши
- Выберите элемент меню ***Сканировать с помощью AVG***, чтобы начать сканирование файла с помощью программы AVG

11.4. Сканирование с помощью командной строки

В **AVG 9.0 File Server** можно выбрать запуск сканирования из командной строки. Например, данный параметр может быть использован на серверах, а также при создании пакетного сценария, запускаемого автоматически при загрузке компьютера. Из командной строки можно запустить сканирование со всеми основными параметрами, доступными в графическом интерфейсе пользователя AVG.

Чтобы запустить сканирование AVG из командной строки, выполните следующую команду в папке установки AVG:

- ***avgscanx*** для 32-разрядной ОС;
- ***avgscana*** для 64-разрядной ОС.

Синтаксис команды

Команда имеет следующий синтаксис.

- ***avgscanx /parameter*** ... например, ***avgscanx /comp*** для сканирования всего компьютера

- ***avgscanx /parameter /parameter*** .. несколько параметров в одной сроке отделяются пробелом и косой чертой,

- если для параметров необходимо указать определенное значение (например, параметр ***/scan***, которому необходимы сведения о том, какие области на компьютере необходимо сканировать, а также прямой путь к выбранному разделу), значения отделяются запятыми, например ***avgscanx /scan=C:\,D:***

Параметры сканирования

Для получения полного списка доступных параметров введите соответствующую команду вместе с параметром /? или /HELP (например, ***avgscanx /?***). Единственный обязательный параметр — /SCAN, который определяет сканируемые области компьютера. Подробное описание параметров см. в обзоре параметров командной строки.

Чтобы начать сканирование, нажмите клавишу ***Enter***. Процесс сканирования можно остановить, нажав сочетание клавиш ***Ctrl+C*** или ***Ctrl+Pause***.

Сканирование из командной строки запущено с помощью графического интерфейса

При запуске компьютера в безопасном режиме Windows также можно запустить сканирование из командной строки с помощью графического интерфейса пользователя. Сканирование запустится из командной строки, диалоговое окно ***Конструктор командной строки*** позволяет определить большинство основных параметров сканирования с помощью удобного графического интерфейса.

Так как данное диалоговое окно доступно только в безопасном режиме Windows, более подробное описание данного окна можно получить в файле справки, доступном непосредственно в этом диалоговом окне.

11.4.1. Параметры сканирования с помощью командной строки

Просмотрите список всех параметров для сканирования командной строки.

- ***/SCAN*** Сканировать отдельные файлы или папки /SCAN=путь; путь (например, /SCAN=C:\;D:\)

- ***/COMP*** Сканирование всего компьютера

- ***/HEUR*** Использовать эвристический анализ
- ***/EXCLUDE*** Исключить путь или файлы из сканирования
- ***/@*** Командный файл /имя файла/
- ***/EXT*** Сканировать эти расширения /например, EXT=EXE,DLL/
- ***/NOEXT*** Не сканировать эти расширения /например, NOEXT=JPG/
- ***/ARC*** Сканировать архивы
- ***/CLEAN*** Автоматическая очистка
- ***/TRASH*** Переместить зараженные файлы в хранилище вирусов
- ***/QT*** Быстрая проверка
- ***/MACROW*** Сообщать о макросах
- ***/PWDW*** Сообщать о файлах, защищенных паролем
- ***/IGNLOCKED*** Пропускать заблокированные файлы
- ***/REPORT*** Отчет в файл /имя файла/
- ***/REPAPPEND*** Добавить в файл отчета
- ***/REPOK*** Сообщать о незараженных файлах
- ***/NOBREAK*** Запретить остановку по нажатию CTRL-BREAK
- ***/BOOT*** Включить проверку сектора MBR/загрузочного сектора
- ***/PROC*** Сканировать активные процессы
- ***/PUP*** Сообщать о "потенциально нежелательных программах"
- ***/REG*** Сканировать реестр
- ***/COO*** Сканировать файлы cookie
- ***/?*** Показать справку по этой теме

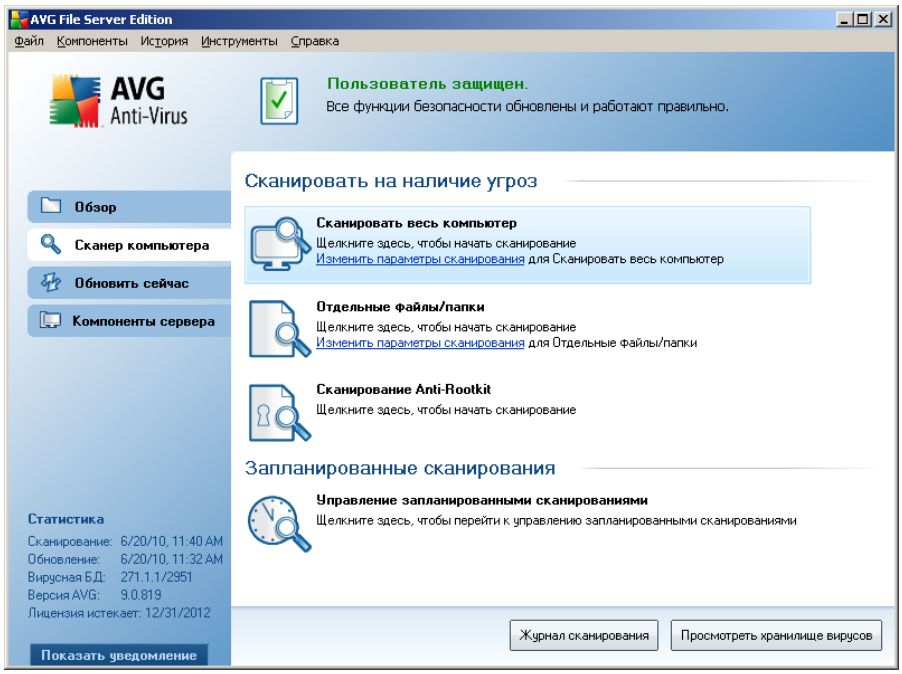
- ***/HELP*** Показать справку по этой теме
- ***/PRIORITY*** Установить приоритет сканирования /Низкий, Автоматически, Высокий/ (см. Дополнительные параметры/Сканирование)
- ***/SHUTDOWN*** Выключить компьютер по завершении сканирования
- ***/FORCESHUTDOWN*** Принудительное выключение компьютера по завершении сканирования
- ***/ADS*** Сканировать альтернативные потоки данных (только NTFS)
- ***/ARCBOMBSW*** Сообщать об "архивных бомбах" (повторно сжатые архивы)

11.5. Расписание сканирования

С помощью **AVG 9.0 File Server** можно запустить сканирование по требованию (в случае предполагаемого заражения компьютера) или запланированное сканирование. Рекомендуется запускать сканирование согласно расписанию. В этом случае вы будете уверены, что компьютер надежно защищен от всех возможных инфекций, и не придется волноваться о том, нужно ли и когда запускать сканирование.

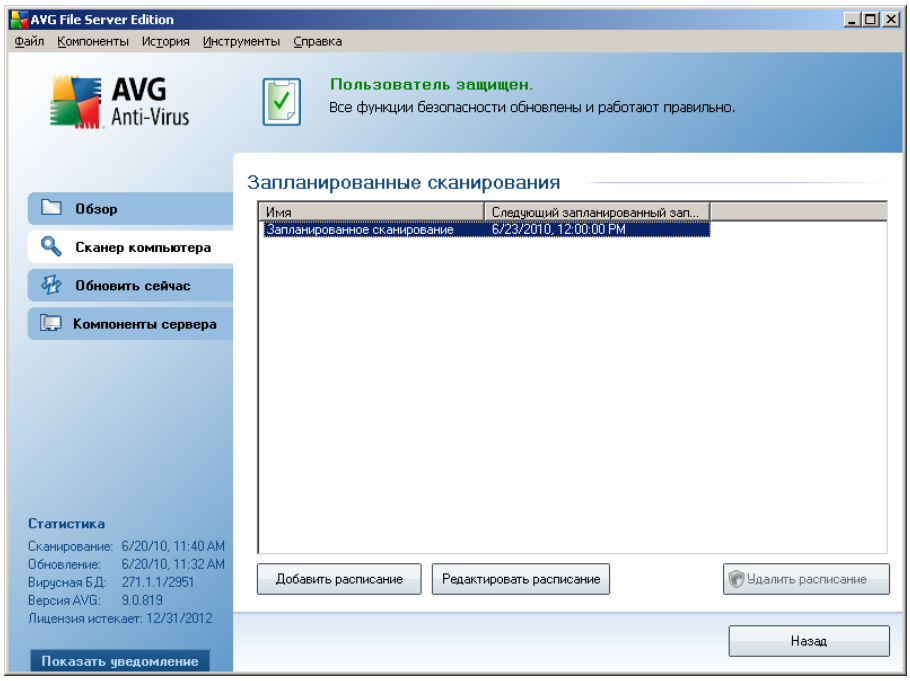
Сканирование всего компьютера необходимо запускать как минимум раз в неделю. Все же, если это возможно, рекомендуется запускать сканирование всего компьютера ежедневно (как настроено в конфигурации расписания сканирования по умолчанию). Если компьютер всегда включен, можно назначить сканирование на нерабочее время. Если пользователь иногда выключает компьютер, сканирование начинается сразу же при включении компьютера, если сканирование в заданное время было пропущено.

Для создания новых расписаний сканирования откройте Интерфейс сканирования AVG и см. раздел ***Запланированные сканирования***, расположенный в нижней части интерфейса сканирования.



Запланированные сканирования

Щелкните графический значок в разделе ***Запланированные сканирования***, чтобы открыть новое диалоговое окно ***Запланированные сканирования***, в котором находится список текущих запланированных сканирований.



Сканирования можно редактировать или добавлять с помощью следующих кнопок управления.

- ***Добавить расписание сканирования***. Открытие диалогового окна ***Параметры запланированного сканирования***, вкладки ***Параметры расписания***. В данном диалоговом окне можно указать параметры новой созданной проверки.

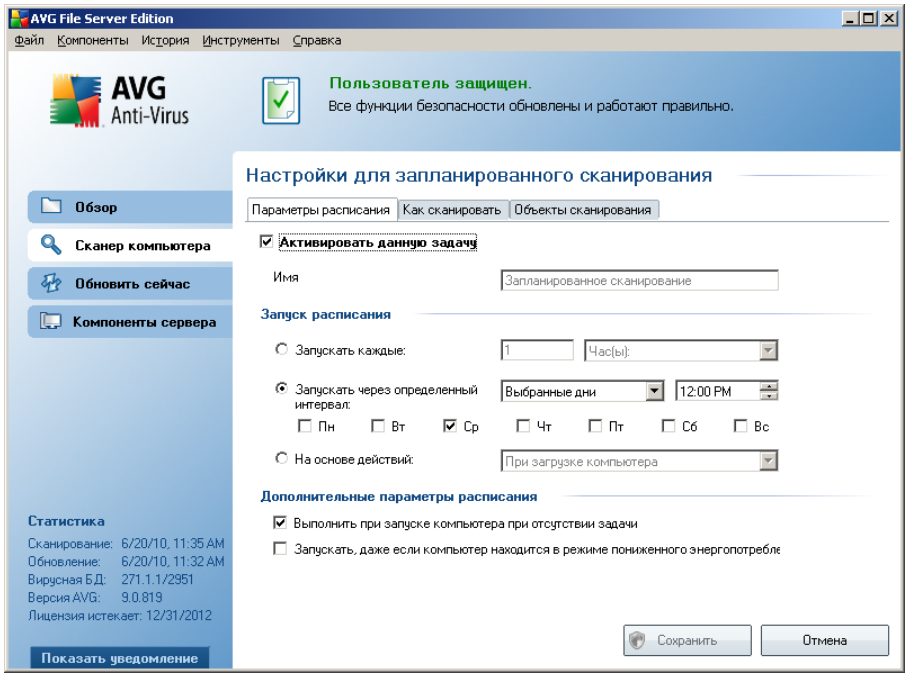
- ***Редактировать расписание сканирования***. Используется, только если текущая проверка была предварительно выбрана в списке запланированных проверок. В данном случае кнопка активна и может использоваться для перехода к диалоговому окну ***Параметры запланированного сканирования***, вкладке ***Параметры расписания***. Параметры выбранной проверки уже указаны и могут быть изменены.

- ***Удалить расписание сканирования***. Данная кнопка также активна, если текущая проверка была предварительно выбрана в списке запланированных проверок. В будущем эту проверку можно удалить из списка с помощью кнопки управления. При этом пользователь может удалять только собственные проверки; удаление ***расписания полного сканирования компьютера***, предварительно определенного параметрами по умолчанию, недоступно.

- ***Назад***. Возврат к интерфейсу сканирования AVG

11.5.1. Параметры расписания

При необходимости запланировать новую проверку и ее регулярный запуск войдите в диалоговое окно ***Параметры запланированной проверки*** (*нажмите кнопку* ***Добавить расписание сканирования*** *в диалоговом окне* ***Запланированные сканирования***). Диалоговое окно содержит три вкладки. ***Параметры расписания*** *(см. рисунок ниже, вкладка по умолчанию, на которую пользователь перенаправляется автоматически*), ***Способы сканирования*** и ***Объекты сканирования***.



На вкладке ***Параметры расписания*** можно сначала установить или снять флажок элемента ***Активировать данную задачу***, чтобы временно отключить запланированную проверку и включить ее при необходимости.

Далее необходимо указать название сканирования, которое будет создано и запланировано. Введите название в текстовое поле рядом с элементом ***Название*** . Старайтесь использовать краткие, содержательные и понятные названия расписаний обновления, так как позже это облегчит их поиск среди остальных расписаний обновления.

Пример. *Названия "Новое сканирование" или "Мое сканирование" не являются*

содержательными, так как не связаны с объектами, которые будут проверяться. И наоборот, название "Сканирование системных областей" является хорошим содержательным названием. Хотя и не обязательно указывать в названии сканирования, является ли оно сканированием всего компьютера или только сканированием выбранных файлов или папок, созданные сканирования будут определяться как разновидности сканирования выбранных файлов и папок.

В данном диалоговом окне можно определить следующие параметры сканирования.

- ***Выполняемое расписание*** — укажите временные интервалы запуска нового запланированного сканирования. Можно определить время запуска сканирования через определенные промежутки времени (***Запускать каждые ...***), указать точные дату и время запуска сканирования (***Запускать в определенное время ...***), а также определить событие, с которым должен быть связан запуск сканирования (***Действие связано с включением компьютера***).

- ***Дополнительные параметры расписания*** — данный раздел позволяет определить условия, при которых должен или не должен выполняться запуск сканирования, если компьютер работает в энергосберегающем режиме или выключен.

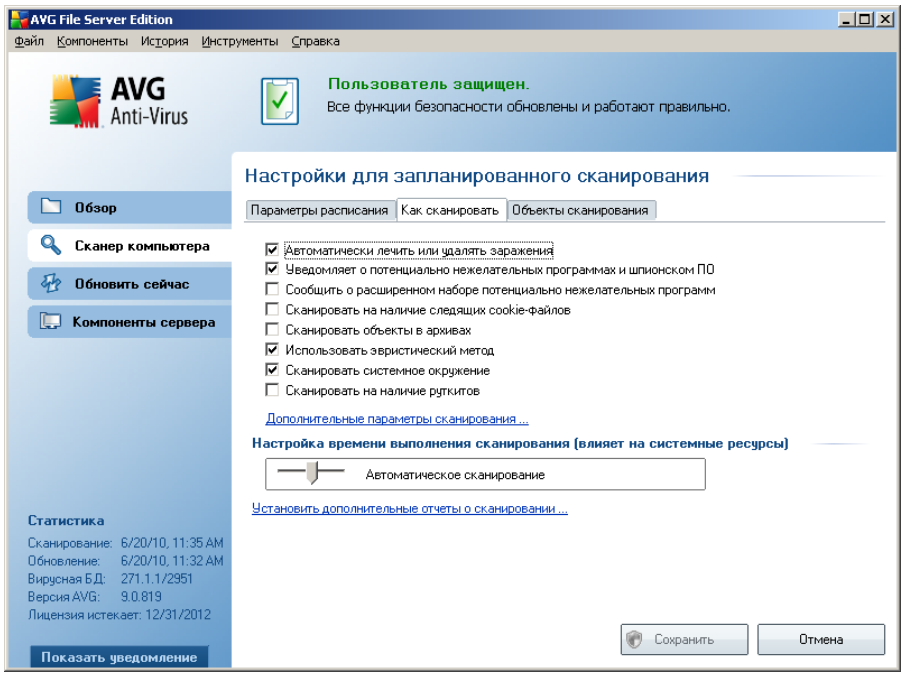
Кнопки управления параметрами диалогового окна запланированного сканирования

На каждой из трех вкладок диалогового окна ***Параметры запланированного сканирования*** (***Параметры расписания***, ***Способы сканирования*** и ***Объекты сканирования***) расположены две кнопки управления, которые имеют одинаковые функции независимо от того, какая вкладка выбрана.

- ***Сохранить***. Сохранение всех изменений, выполненных на этой или другой вкладке данного диалогового окна, а также обратный переход к стандартному диалоговому окну интерфейса сканирования AVG. Следовательно, при необходимости настроить на вкладках параметры проверки, нажимайте кнопку для их сохранения только после указания всех необходимых параметров.

- ***Отмена*** . Отмена любых изменений, выполненных на этой или других вкладках данного диалогового окна, а также возврат к диалоговому окну по умолчанию интерфейса сканирования AVG.

11.5.2. Способы сканирования



На вкладке ***Способ сканирования*** приведен список параметров сканирования, которые при необходимости можно включить или отключить. По умолчанию большинство параметров включены и используются при сканировании. Если нет веских оснований для изменения данных параметров, рекомендуется не изменять стандартные настройки.

- ***Автоматически лечить или удалять заражения***. Обнаруженный при сканировании вирус будет вылечен автоматически, если лечение возможно. Если зараженный файл невозможно вылечить автоматически или данный параметр отключен, отобразится уведомление об обнаружении вируса с выбором действия по отношению к зараженному объекту. Рекомендуется переместить зараженный файл в ***хранилище вирусов***.

- ***Уведомлять о потенциально нежелательных программах и угрозах появления шпионского ПО***. Данный параметр управляет функциями компонента ***Anti-Virus***, которые позволяют обнаруживать потенциально нежелательные программы (*исполняемые файлы, которые могут работать в качестве шпионского или рекламного ПО*), блокировать их или удалять.

- ***Уведомлять о расширенном наборе потенциально нежелательных программ***. Обнаружение расширенного пакета шпионского ПО: программы, которые полностью безопасны и не вызывают подозрений при

приобретении у производителя, но могут представлять угрозу при использовании злоумышленниками. Данный параметр является дополнительной мерой, еще больше повышающей уровень безопасности, однако из-за него могут также блокироваться некоторые законные программы, поэтому по умолчанию параметр отключен.

- ***Сканировать на наличие следящих файлов cookie***. Данный параметр компонента ***Anti-Spyware*** включает сканирование системы на наличие файлов cookie *(файлы cookie протокола HTTP используются для аутентификации, отслеживания и сохранения определенной информации о пользователях, например о предпочитаемых сайтах или содержимом корзин для покупок через Интернет*).

- ***Сканировать объекты в архивах***. Данный параметр означает, что при сканировании должны быть проверены все файлы, даже те, которые находятся в архивах некоторых типов, например ZIP, RAR и других.

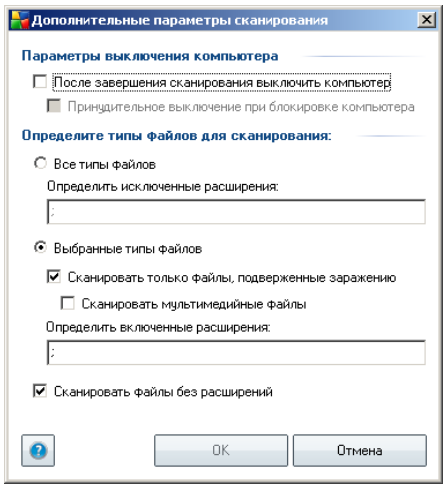
- ***Использовать эвристический анализ***. Эвристический анализ (*динамичная эмуляция команд сканированных объектов в виртуальной компьютерной среде*) является одним из способов, используемых для выявления вирусов при сканировании.

- ***Сканировать системную среду***. При сканировании будут также проверяться системные области компьютера.

- ***Сканировать на наличие rootkits***. Установите этот флажок, чтобы искать средства rootkit при сканировании всего компьютера. Определение средств rootkit можно выполнить отдельно с помощью компонента ***Anti-Rootkit***.

Затем, чтобы изменить параметры сканирования, выполните следующие действия.

- ***Дополнительные параметры сканирования***. Эта ссылка открывает новое диалоговое окно ***Дополнительные параметры сканирования***, где можно указывать следующие параметры.



- ***Параметры выключения компьютера***. Определяет, необходимо ли автоматическое выключение компьютера после завершения процесса сканирования. После выбора этого параметра (***Выключить компьютер после завершения сканирования***) становится доступен новый параметр, позволяющий выключать компьютер, даже если он заблокирован (***Принудительное выключение при блокировке компьютера***).

- ***Определение типов файлов для сканирования***. Далее необходимо указать типы файлов для сканирования.

  - ***Все типы файлов*** с возможностью определения исключений из сканирования посредством предоставления списка расширений файлов, разделенных запятыми, сканирование которых проводиться не будет.

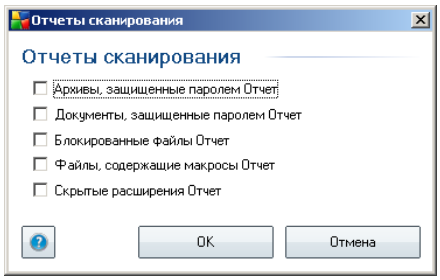
  - ***Выбранные типы файлов***. Можно указать сканирование только тех файлов, которые подвержены заражению (*файлы, не подверженные заражению, не будут сканироваться, например простые текстовые файлы или другие неисполняемые файлы*), включая мультимедийные файлы (*видео- и аудиофайлы — если не устанавливать этот флажок, время сканирования значительно уменьшится, так как эти файлы обладают довольно большим размером и вероятность их заражения вирусом мала*). С помощью расширений можно указать файлы, которые необходимо сканировать всегда.

  - Дополнительно можно установить флажок ***Сканировать файлы без расширений***. Он установлен по умолчанию. Рекомендуется

не изменять его без веских причин. Файлы без расширения являются подозрительными, поэтому необходимо выполнять их сканирование каждый раз.

- ***Приоритет процесса сканирования***. Для изменения приоритета процесса сканирования используйте ползунок. По умолчанию установлен средний уровень приоритета (*Автоматическое сканирование*), который обеспечивает оптимальную скорость процессора и использование системных ресурсов. Также можно запустить процесс сканирования на медленной скорости, чтобы снизить нагрузку на системные ресурсы (*рекомендуется, если пользователю не важно, как долго выполняется сканирование*), или на быстрой с большим потреблением системных ресурсов (*например, если компьютер временно не используется*).

- ***Настроить дополнительные отчеты сканирования***. При нажатии этой ссылки открывается диалоговое окно ***Отчеты сканирования***, в котором можно выбрать типы объектов, сведения о которых должны отображаться в отчете.



Примечание. *По умолчанию установлена конфигурация для достижения оптимальной производительности при сканировании. Не рекомендуется изменять стандартные параметры сканирования без необходимости. Любые изменения параметров должны выполнять только опытные пользователи. Дополнительные параметры конфигурации сканирования находятся в диалоговом окне* ***Дополнительные параметры****, доступ к которому можно получить с помощью элементов системного меню* ***Файл/Дополнительные параметры****.*

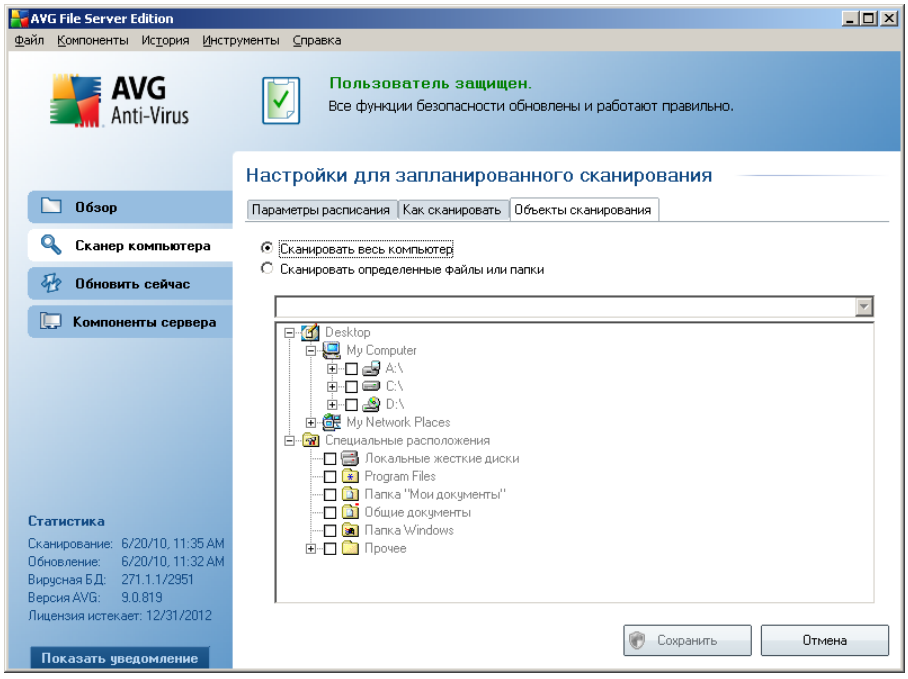
Кнопки управления

На каждой из трех вкладок (***Параметры расписания***, ***Способы сканирования*** ***и*** Объекты сканирования***) диалогового окна*** ***Параметры запланированного сканирования*** расположены две кнопки управления, которые имеют одинаковые функции независимо от того, какая вкладка выбрана.

- ***Сохранить***. Сохранение всех изменений, выполненных на этой или другой вкладке данного диалогового окна, а также обратный переход к стандартному диалоговому окну интерфейса сканирования AVG. Следовательно, при необходимости настроить на вкладках параметры проверки, нажимайте кнопку для их сохранения только после указания всех необходимых параметров.

- ***Отмена*** . Отмена любых изменений, выполненных на этой или других вкладках данного диалогового окна, а также возврат к диалоговому окну по умолчанию интерфейса сканирования AVG.

11.5.3. Объекты сканирования



На вкладке ***Объекты сканирования*** можно запланировать сканирование всего компьютера или сканирование отдельных файлов и папок. Если выбрать сканирование определенных файлов и папок, в нижней части этого диалогового окна активируется отображаемая структура дерева, где можно указать папки, сканирование которых необходимо выполнить.

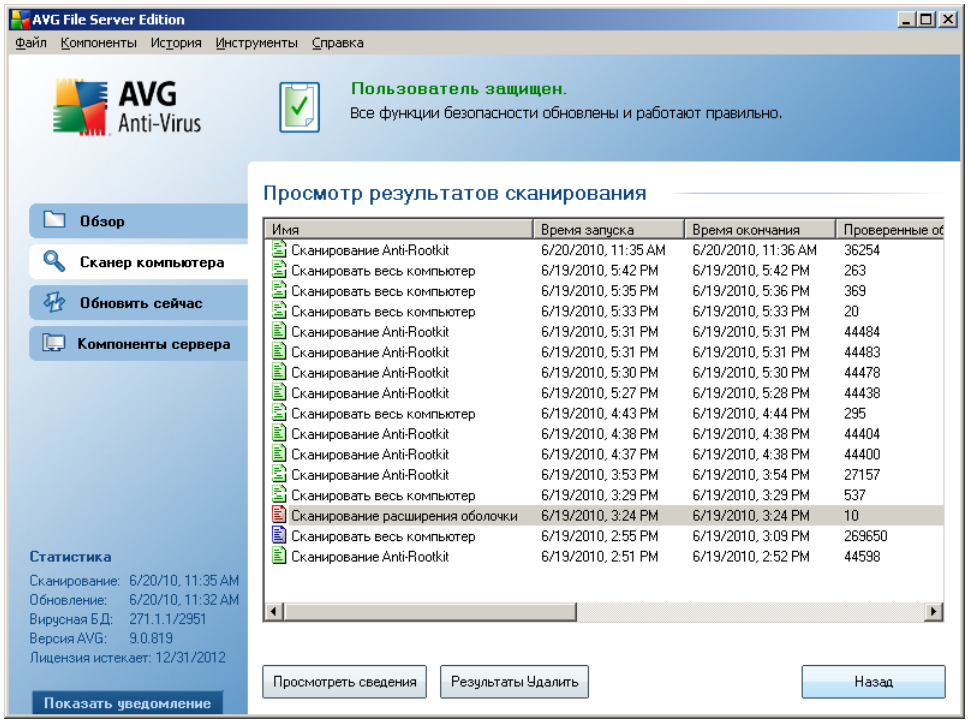
Кнопки управления параметрами диалогового окна запланированного сканирования

На каждой из трех вкладок диалогового окна ***Параметры запланированного сканирования*** (***Параметры расписания***, ***Способы сканирования*** и ***Объекты сканирования***) расположены две кнопки управления, которые имеют одинаковые функции независимо от того, какая вкладка выбрана.

- ***Сохранить***. Сохранение всех изменений, выполненных на этой или другой вкладке данного диалогового окна, а также обратный переход к стандартному диалоговому окну интерфейса сканирования AVG. Следовательно, при необходимости настроить на вкладках параметры проверки, нажимайте кнопку для их сохранения только после указания всех необходимых параметров.

- ***Отмена*** . Отмена любых изменений, выполненных на этой или других вкладках данного диалогового окна, а также возврат к диалоговому окну по умолчанию интерфейса сканирования AVG.

11.6. Обзор результатов сканирования



Диалоговое окно ***Обзор результатов сканирования*** можно просмотреть, нажав в интерфейсе сканирования AVG кнопку ***Журнал сканирования***. В данном диалоговом окне приводится список всех запущенных ранее процессов

сканирования, а также сведения о полученных результатах.

- ***Имя*** — наименование сканирования; это может быть предварительно определенное название сканирования или пользовательское наименование запланированного сканирования. Рядом с каждым именем отображается значок, обозначающий результат сканирования:

   — зеленый значок отображается, если при сканировании не было обнаружено заражений

   — синий значок отображается, если при сканировании были обнаружены заражения, но зараженные объекты были автоматически удалены

   — красный значок отображается, если при сканировании были обнаружены заражения, но не удалось удалить зараженные объекты

  Значки могут быть цельными или разделенными — цельные значки обозначают сканирования, которые были полностью завершены; разделенные значки обозначают отмененные или прерванные сканирования.

  Примечание. *Подробные сведения об операциях сканирования см. в диалоговом окне* ***Результаты сканирования****, доступном при нажатии кнопки* ***Просмотреть сведения*** *(в нижней части данного диалогового окна).*

- ***Время запуска*** — дата и время запуска процесса сканирования
- ***Время окончания*** — дата и время завершения процесса сканирования
- ***Проверенные объекты*** — количество объектов, проверенных в процессе сканирования
- ***Вирусы***. Количество обнаруженных и удаленных вирусов
- ***Шпионское ПО***. Количество обнаруженных и удаленных объектов шпионского ПО.
- ***Сведения журнала сканирования*** — сведения, связанные с процессом и результатами сканирования (обычно при завершении или прерывании процесса сканирования)

Кнопки управления

В диалоговом окне ***Обзор результатов сканирования*** доступны следующие кнопки управления.

- ***Просмотреть сведения*** — данная кнопка активна, только если в обзоре выше выбрано определенное сканирование; нажмите эту кнопку, чтобы открыть окно ***Результаты сканирования*** для просмотра подробных сведений о выбранном сканировании
- ***Удалить результат*** — данная кнопка активна, только если в обзоре выше выбрано определенное сканирование; нажмите эту кнопку, чтобы удалить выбранный объект в окне результатов сканирования
- ***Назад***. Данная кнопка служит для повторного открытия диалогового окна интерфейса сканирования AVG

11.7. Сведения о результатах сканирования

Если в диалоговом окне ***Обзор результатов сканирования*** выбрано определенное сканирование, можно нажать кнопку ***Просмотреть сведения*** для перехода к диалоговому окну ***Результаты сканирования***. В данном окне приведены подробные сведения о процессе и результате выбранного сканирования.

Данное диалоговое окно состоит из нескольких вкладок.

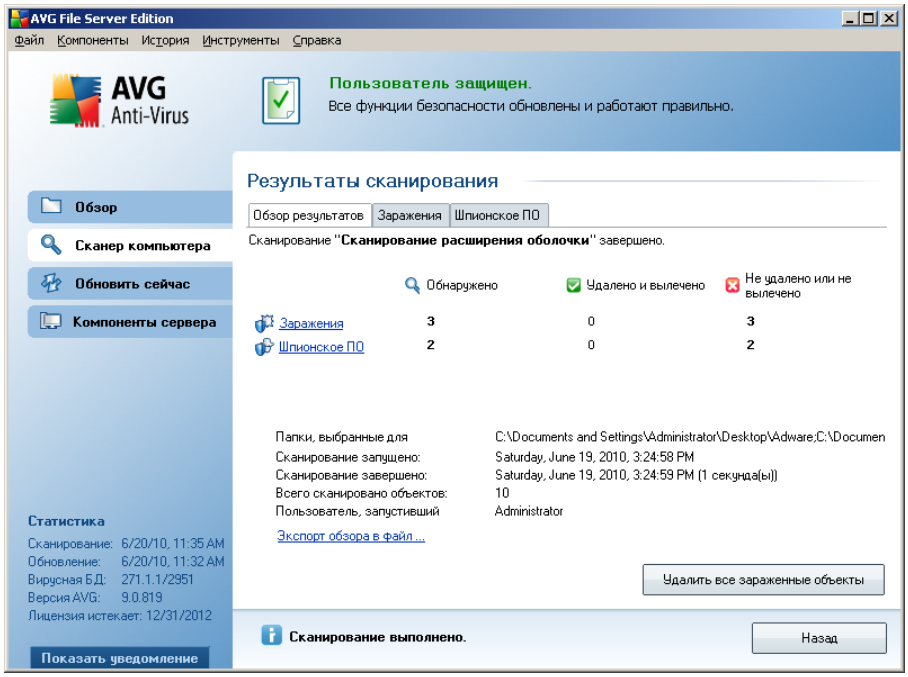
- ***Обзор результатов***. Данная вкладка отображается каждый раз при выполнении сканирования и предоставляет статистические данные с описанием процесса сканирования.
- ***Заражения***. Данная вкладка отображается только в том случае, если во время сканирования было обнаружено заражение вирусом.
- ***Шпионское ПО***. Данная вкладка отображается только в том случае, если во время сканирования было обнаружено шпионское ПО.
- ***Предупреждения*** — данная вкладка отображается только в том случае, если во время сканирования были обнаружены объекты, сканирование

которых недоступно

- ***Rootkit***. Данная вкладка отображается только в том случае, если во время сканирования были обнаружены средства rootkit.

- ***Сведения*** — данная вкладка отображается только в том случае, если были обнаружены потенциальные угрозы, не подпадающие ни под одну из перечисленных выше категорий; в данном случае на вкладке отображается предупреждающее сообщение об обнаружении

11.7.1. Вкладка "Обзор результатов"



На вкладке ***Результаты сканирования*** содержатся следующие подробные статистические сведения:

- обнаруженные вирусы/шпионское ПО/предупреждения/rootkits/информация

- удаленные заражения вирусами/шпионское ПО/предупреждения/rootkits

- количество заражений вирусами/шпионского ПО/предупреждений/rootkits, которые не удалось удалить или вылечить

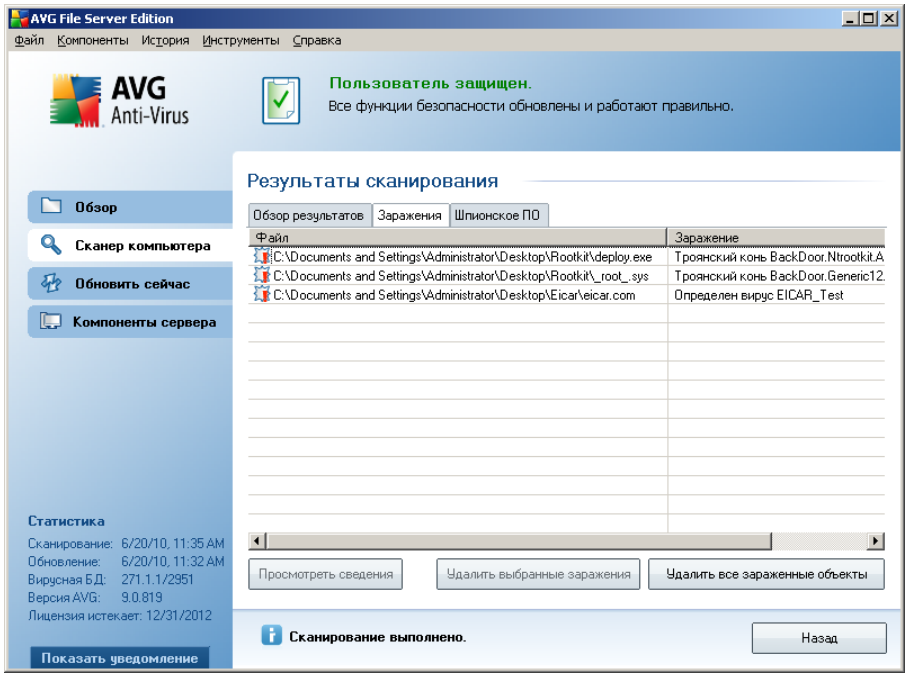
Кроме того, здесь содержится информация о дате и точном времени запуска

сканирования, общем количестве сканированных объектов, продолжительности сканирования, количестве ошибок, произошедших при сканировании, и пользователе, запустившем сканирование.

Кнопки управления

В данном диалоговом окне доступно только две кнопки управления. Кнопка ***Закрыть результаты*** обеспечивает переход обратно к диалоговому окну ***Обзор результатов сканирования***. Кнопка ***Удалить все зараженные объекты, лечение которых невозможно*** отображается только в том случае, если при сканировании были обнаружены угрозы, которые не были удалены автоматически. При нажатии кнопки такие угрозы будут перемещены в ***хранилище вирусов***.

11.7.2. Вкладка "Заражения"



Вкладка ***Заражения*** отображается в диалоговом окне ***Результаты сканирования*** только в том случае, если во время сканирования было обнаружено заражение вирусом. Вкладка разделена на три части, содержащие следующие данные.

- ***Файл***. Полный путь к исходному местоположению зараженного объекта.

- ***Зараженный объект***. Имя обнаруженного вируса (*подробные сведения об определенных вирусах см. в интерактивной энциклопедии вирусов*).

- ***Результат***. Определение текущего состояния объекта, обнаруженного при сканировании.

    - ***Заражен***. Зараженный объект обнаружен, его начальное местоположение сохранено (*например, если в специальных параметрах сканирования отключен параметр автоматического лечения*).

    - ***Вылечен***. Зараженный объект вылечен автоматически, его начальное местоположение сохранено.

    - ***Перемещен в хранилище вирусов***. Зараженный объект помещен на карантин в ***хранилище вирусов***.

    - ***Удален***. Зараженный объект удален.

    - ***Добавлен в список исключений PUP***. Обнаруженный объект получил статус исключения и был добавлен в список исключений PUP (*настроенный в диалоговом окне* ***Исключения PUP*** *дополнительных параметров*).

    - ***Заблокированный файл — не проверен***. Объект заблокирован, поэтому AVG не может выполнить его сканирование.

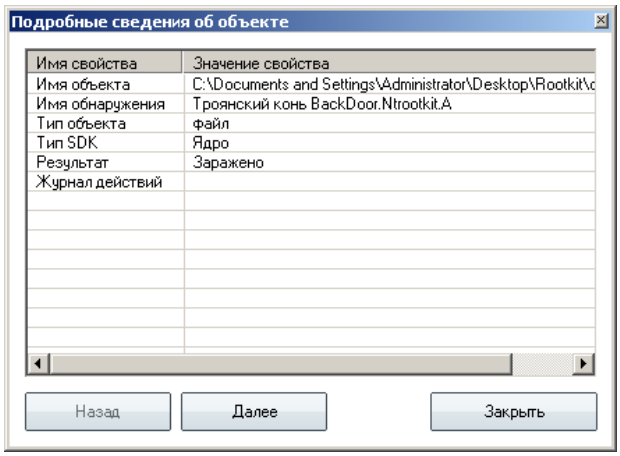
    - ***Потенциально опасный объект***. Объект является потенциально опасным, но не заражен (*например, содержит макросы*); данная информация имеет лишь предупредительный характер.

    - ***Для завершения процесса требуется перезагрузка***. Невозможно удалить зараженный объект; необходимо перезагрузить компьютер, чтобы полностью удалить объект.

Кнопки управления

В данном диалоговом окне доступны три кнопки управления.

- ***Просмотреть сведения***. В результате нажатия данной кнопки открывается новое диалоговое окно ***Подробная информация об объектах***.



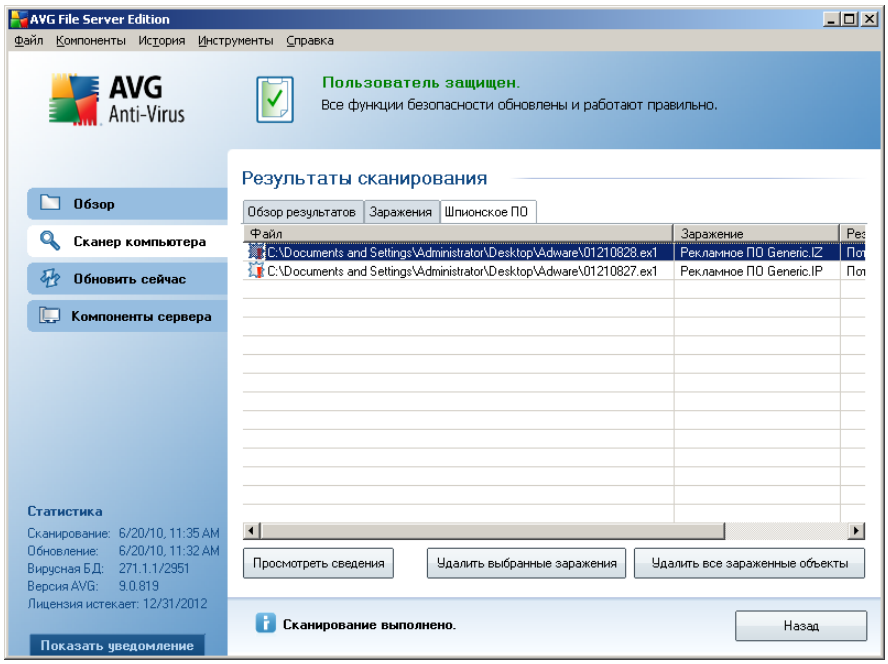
В данном диалоговом окне приведена информация о местоположении обнаруженного зараженного объекта (***Имя свойства***). С помощью кнопок ***Назад***/***Далее*** можно просматривать сведения об определенных обнаруженных объектах. Чтобы закрыть диалоговое окно, нажмите кнопку ***Закрыть***.

- ***Удалить выбранные заражения***. Используйте эту кнопку, чтобы вылечить выбранные обнаруженные заражения или переместить их в ***хранилище вирусов*** (если не удается вылечить).

- ***Удалить все зараженные объекты, лечение которых невозможно***. Используйте эту кнопку, чтобы вылечить все обнаруженные заражения в списке или переместить их в ***хранилище вирусов*** (если не удается вылечить).

- ***Закрыть результаты***. Закрытие окна просмотра сведений и возврат к окну ***Просмотр результатов сканирования***.

11.7.3. Вкладка "Шпионское ПО"



Вкладка ***Шпионское ПО*** отображается в диалоговом окне ***Результаты сканирования***, только если при сканировании было обнаружено шпионское программное обеспечение. Вкладка разделена на три части, содержащие следующие данные.

- ***Файл***. Полный путь к исходному местоположению зараженного объекта.
- ***Зараженный объект***. Имя обнаруженного шпионского ПО (*подробные сведения об определенных вирусах см. в интерактивной* ***энциклопедии вирусов***).
- ***Результат***. Определяет текущее состояние объекта, обнаруженного при сканировании.
    - ***Заражен***. Зараженный объект обнаружен, его начальное местоположение сохранено (например, если в особых настройках сканирования отключен параметр автоматического лечения).
    - ***Вылечен***. Зараженный объект вылечен автоматически, его начальное местоположение сохранено.

- ***Перемещен в хранилище вирусов***. Зараженный объект помещен на карантин в ***хранилище вирусов*** .

- ***Удален***. Зараженный объект удален.

- ***Добавлен в список исключений PUP***. Обнаруженный объект получил статус исключения и добавлен в список исключений PUP (*настроенный в диалоговом окне дополнительных параметров Исключения PUP*).

- ***Заблокированный файл — не проверен***. Объект заблокирован, поэтому AVG не может выполнить его сканирование.

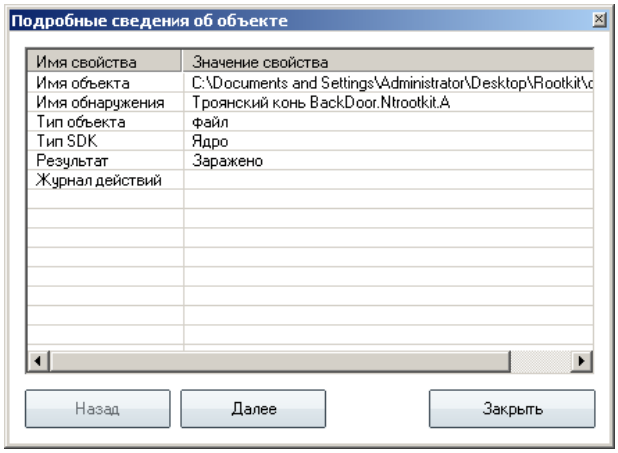
- ***Потенциально опасный объект***. Объект является потенциально опасным, но не заражен (например, содержит макросы); данная информация имеет лишь предупредительный характер.

- ***Для завершения процесса требуется перезагрузка***. Невозможно удалить зараженный объект; необходимо перезагрузить компьютер, чтобы полностью удалить объект.

Кнопки управления

В данном диалоговом окне доступны три кнопки управления.

- ***Просмотреть сведения***. При нажатии данной кнопки открывается новое диалоговое окно с указанным именем ***Подробная информация о результатах сканирования***.



В данном диалоговом окне приведена информация о местоположении обнаруженного зараженного объекта (***Имя свойства***). С помощью кнопок ***Назад***/***Далее*** можно просматривать сведения об определенных обнаруженных объектах. Чтобы закрыть диалоговое окно, нажмите кнопку ***Закрыть***.

- ***Удалить выбранные заражения***. Используйте эту кнопку, чтобы вылечить выбранные обнаруженные заражения или переместить их в ***хранилище вирусов*** (если не удается вылечить).

- ***Удалить все зараженные объекты, лечение которых невозможно***. Используйте эту кнопку, чтобы вылечить все обнаруженные заражения в списке или переместить их в ***хранилище вирусов*** (если не удается вылечить).

- ***Закрыть результаты***. Закрытие окна просмотра сведений и возврат к окну ***Просмотр результатов сканирования***.

11.7.4. Вкладка "Предупреждения"

Вкладка ***Предупреждения*** содержит сведения о подозрительных объектах (*обычно это файлы*), обнаруженных при сканировании. При обнаружении компонентом ***Resident Shield*** доступ к данным файлам блокируется. Типичные примеры данных объектов: скрытые файлы, файлы cookie, подозрительные ключи реестра, защищенные паролем документы или архивы, а также некоторые другие объекты. Данные файлы не представляют прямой угрозы компьютеру или безопасности. Сведения о данных файлах могут быть полезны в случае обнаружения на компьютере шпионского или рекламного ПО. Если при проверке AVG выводятся только предупреждения, не требуется предпринимать каких-либо действий.

Ниже приведено краткое описание наиболее распространенных подозрительных объектов.

- ***Скрытые файлы*** — файлы, которые по умолчанию не отображаются в ОС Windows. Поэтому некоторые вирусы и другие угрозы могут попытаться избежать обнаружения, присвоив своим файлам атрибут "Скрытый". Если программа AVG сообщает об обнаружении скрытого файла, который кажется подозрительным, его можно переместить в ***хранилище вирусов AVG***.

- ***Файлы cookie*** — это обычные текстовые файлы, используемые веб-сайтами для хранения определенной информации о пользователе, которая используется для последующей загрузки пользовательской компоновки веб-сайта, автоматического ввода имени пользователя и для других целей.

- ***Подозрительные ключи реестра***. Некоторое вредоносное ПО размещает информацию в реестре Windows, чтобы обеспечить загрузку ПО при запуске ОС, а также для расширения своего воздействия на операционную систему.

11.7.5. Вкладка Rootkits

Вкладка ***Rootkits*** содержит информацию о rootkits, обнаруженных при сканировании, если было запущено ***сканирование Anti-Rootkit***.

Rootkit — это программа, предназначенная для полного управление системой компьютера без разрешения владельцев систем или законных управляющих. Средствам rootkit обычно не требуется доступ к оборудованию, так как они предназначены для управления операционными системами, установленными на этом оборудовании. В большинстве случаев средства rootkit скрывают свое присутствие в системе с помощью замены информации или обхода стандартных механизмов безопасности операционных систем. Кроме того, они могут попадать на компьютер в виде троянских программ, которые пользователи уверенно запускают, не подозревая об опасности. Используемые для этого технические приемы включают в себя скрытие запущенных процессов от следящих программ, а файлов и системных данных — от операционных систем.

Структура данной вкладки идентична структуре вкладок ***Заражения*** или ***Шпионское ПО***.

11.7.6. Вкладка "Сведения"

На вкладке ***Сведения*** содержатся данные о найденных объектах, которые не удалось отнести к доступным категориям (заражения, шпионское ПО и т. п.). Данные объекты не были отмечены как "опасные", но они являются подозрительными. Сканирование AVG позволяет определять файлы, которые могут быть не заражены, но являются подозрительными. Сообщение о таких файлах отображается в виде ***предупреждения*** или ***сведений***.

Сообщения со ***сведениями*** об уровне опасности отображаются в следующих случаях.

- ***Упаковывание в среде выполнения*** — упаковывание файла с помощью нераспространенного упаковщика среды выполнения, что может указывать на попытку предотвращения сканирования такого файла. Однако не каждое сообщение о таком файле указывает на наличие вируса.

- ***Рекурсивное упаковывание в среде выполнения*** — случай, похожий на описанный выше, но встречающийся реже при использовании распространенного ПО. Такие файлы являются подозрительными и могут быть удалены или отправлены на анализ.

- ***Архив или документ, защищенные паролем*** — файлы, защищенные паролем, не могут быть проверены программой AVG (*или другой антивирусной программой*)

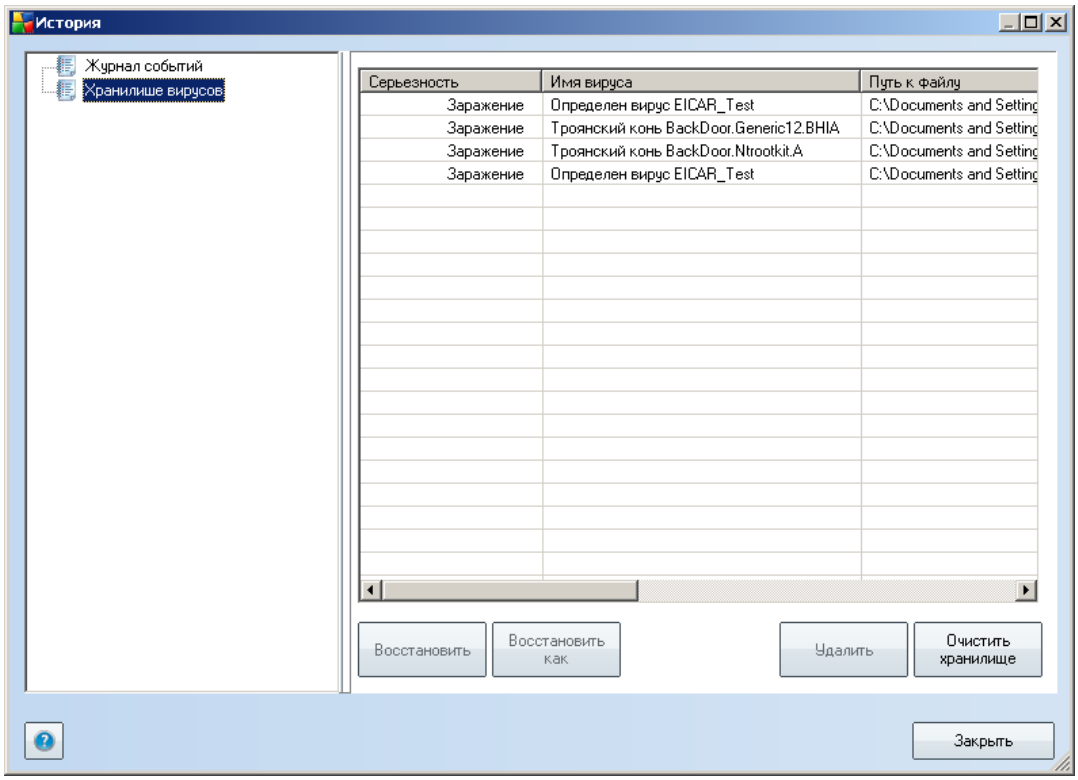
- ***Документ, содержащий макросы*** — документ, указанный в отчете, содержит макросы, которые могут быть вредоносными.

- ***Скрытое расширение*** — файлы со скрытым расширением могут отображаться, например как изображения, но в действительности являться исполняемыми файлами (*например, изображение.jpg.exe*). Второе расширение не отображается в ОС Windows по умолчанию, и программа AVG отправляет отчет о таких файлах, чтобы предотвратить их случайное открытие.

- ***Неправильный путь к файлу{*** — если при запуске некоторых важных системных файлов используется путь, отличный от пути по умолчанию (*например, файл winlogon.exe запускается не из папки Windows*), программа AVG сообщает о таком расхождении. В некоторых случаях вирусы используют имена стандартных системных процессов, чтобы скрыть свое присутствие в системе.

- ***Заблокированные файлы*** — если файл, о котором было сообщено, заблокирован, программа AVG не сможет выполнить его проверку. Обычно это означает, что некоторые файлы в настоящий момент используются системой (*например, файл подкачки*).

11.8. Хранилище вирусов



Хранилище вирусов — это безопасная среда для управления зараженными или подозрительными объектами во время проведения тестов AVG. При обнаружении во время сканирования зараженного объекта, который программе AVG не удалось вылечить автоматически, отобразится запрос на выбор дальнейших действий в отношении данного объекта. Рекомендуется переместить объект в ***хранилище вирусов*** для дальнейшего лечения.

Интерфейс ***хранилища вирусов*** открывается в отдельном окне и предоставляет обзор сведений о зараженных объектах, помещенных в карантин.

- ***Серьезность***. Серьезность и тип обнаруженного зараженного объекта.
- ***Тип заражения***. Распознавание обнаруженных типов на основе их уровня заражения (*все объекты в списке могут быть фактически или потенциально заражены*).
- ***Имя вируса***. Имя обнаруженного заражения в соответствии с

энциклопедией вирусов (в Интернете).

- ***Путь к файлу***. Полный путь к исходному местоположению зараженного объекта.
- ***Исходное имя объекта***. В процессе сканирования всем объектам, заносимым в список, программа AVG присваивает стандартное имя. Если же объект имел свое известное исходное имя (*например, имя вложения электронной почты, не соответствующее фактическому содержимому вложения*), оно отобразится в данном столбце.
- ***Дата хранения***. Дата и время обнаружения подозрительного файла и его перемещения в ***хранилище вирусов***

Кнопки управления

В интерфейсе ***хранилища вирусов*** доступны следующие кнопки управления.

- ***Восстановить***. Перемещение зараженного файла в исходное местоположение на диске.
- ***Восстановить как***. Данная кнопка позволяет переместить обнаруженный зараженный объект из ***хранилища вирусов*** в выбранную папку. При этом обнаруженные и подозрительные объекты сохраняются со своими исходными именами. Если исходное имя неизвестно, будет использоваться стандартное имя.
- ***Удалить***. Полное удаление зараженного файла из ***хранилища вирусов***.
- ***Очистить хранилище***. Удаление всех файлов из ***хранилища вирусов***.

12. Обновления AVG

Важно регулярно обновлять приложение AVG, чтобы быть уверенным, что все новые вирусы будут сразу же обнаружены. Так как обновления AVG не выпускаются согласно какому-либо точному расписанию, а скорее в ответ на количество и опасность появляющихся новых угроз, рекомендуется выполнять проверку на наличие обновлений как минимум раз в день. Проверка наличия обновлений каждые 4 часа обеспечивает актуальное состояние вирусной базы AVG в течение дня.

12.1. Уровни обновлений

Существует два уровня обновлений AVG.

- ***Обновление определений***. Содержит изменения, необходимые для надежной антивирусной защиты. Как правило, сюда не включены изменения кода, а только обновления базы данных определений. Обновление необходимо выполнять сразу после его выпуска.
- ***Обновление программы***. Содержит различные изменения, исправления и улучшения программы.

При определении параметров расписания обновления можно указать уровень приоритета для загрузки и установки обновлений.

12.2. Типы обновлений

Существует два типа обновлений.

- ***Обновление по запросу***. Представляет собой мгновенное обновление продукта AVG, которое может быть выполнено в любое время.
- ***Запланированное обновление***. В AVG также можно предварительно настраивать план обновления. После чего запланированное обновление будет периодически выполняться в соответствии с установленными параметрами. При появлении новых файлов обновления в указанном местоположении они будут загружены непосредственно из Интернета или из сетевого каталога. Если обновления недоступны, никакие действия не будут выполняться.

12.3. Процесс обновления

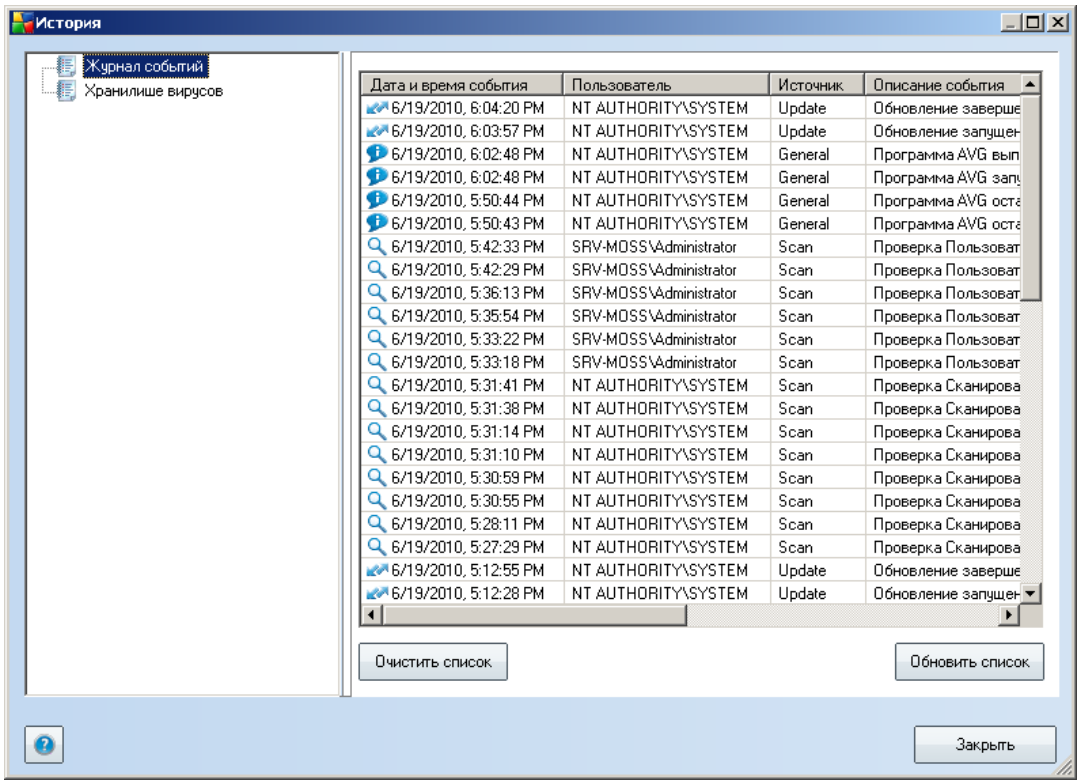
Процесс обновления может быть запущен сразу, как только потребуется, с помощью быстрой ссылки ***Обновить сейчас***. Данная ссылка всегда доступна в диалоговом окне Интерфейс пользователя AVG. Тем не менее, настоятельно

рекомендуется регулярно выполнять обновления по расписанию, которое можно изменить с помощью компонента Диспетчер обновления.

После подтверждения начала обновления программа AVG сначала проверит наличие новых доступных файлов обновления. Если файлы имеются, AVG начнет их загрузку и выполнит запуск обновления самостоятельно. В процессе обновления откроется интерфейс ***Обновление***, где можно увидеть выполняемый процесс в графическом представлении, а также просмотреть соответствующие статистические параметры (*размер файла обновления, полученные данные, скорость загрузки, время выполнения и т. п.*).

***Примечание**. Перед запуском обновления программы AVG создается точка восстановления системы. Если не удастся выполнить обновление или произойдет сбой в работе ОС, всегда можно будет восстановить начальную конфигурацию ОС с этой точки. Данный параметр доступен в меню Пуск/Все программы/ Стандартные /Служебные/Восстановление системы. Однако любые изменения следует вносить только опытным пользователям.*

13. Журнал событий



Диалоговое окно ***История событий*** доступно в системном меню при выборе элементов ***История/Журнал истории событий***. В этом окне можно посмотреть перечень важных событий, произошедших во время работы **AVG 9.0 File Server**. В журнале ***История событий*** регистрируются следующие типы событий.

- Сведения об обновлениях приложения AVG
- Начало, завершение или приостановка процесса сканирования (включая автоматические тесты)
- События, связанные с обнаружением вирусов (компонентом Resident Shield или при сканировании), включая местонахождение угрозы
- Другие важные события

Кнопки управления

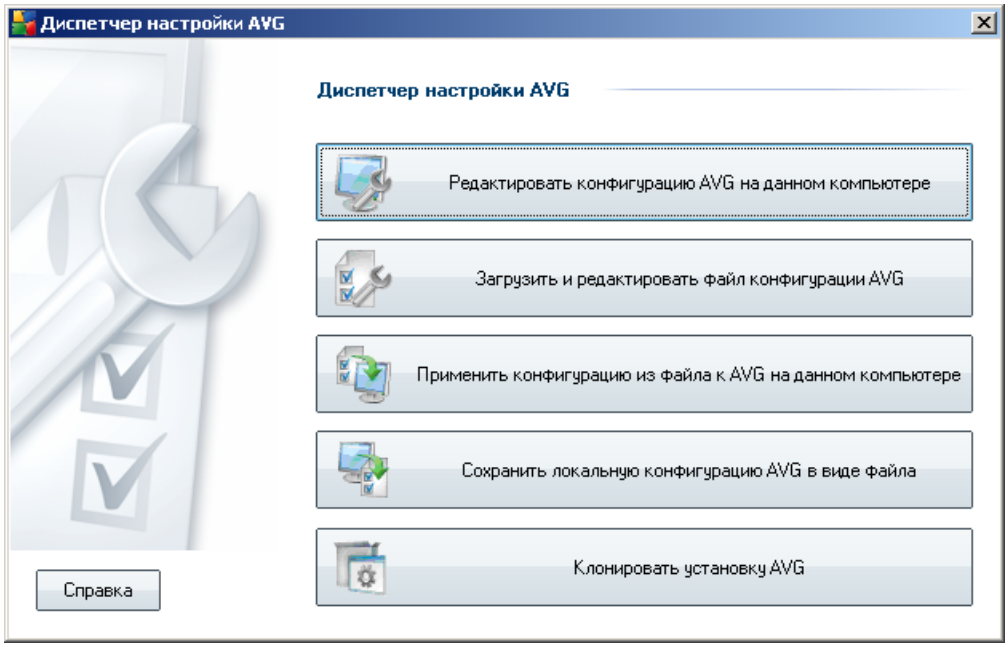
- ***Очистить список*** — удаляет все записи из списка событий
- ***Обновить список*** — обновляет все записи в списке событий

14. Диспетчер параметров AVG

Диспетчер параметров AVG — это инструмент, предназначенный в основном для небольших сетей и позволяющий копировать, редактировать и распределять конфигурацию AVG. Конфигурацию можно сохранить на портативном устройстве (флэш-накопитель USB и т. п.), а затем применить вручную к выбранным станциям.

Данный инструмент включен в пакет установки программы AVG и доступен для запуска в меню ОС Windows Пуск:

Все программы/AVG 9.0/Диспетчер параметров AVG



- ***Изменить конфигурацию AVG на данном компьютере***

  Данная кнопка позволяет открыть диалоговое окно, содержащие расширенные параметры локальной версии программы AVG. Все произведенные в нем изменения будут применены к локальной версии программы AVG.

- ***Загрузить и изменить файл конфигурации AVG***

  Нажмите данную кнопку для редактирования файла конфигурации AVG (.pck) при его наличии. После подтверждения изменений нажмите кнопку ***OK*** или

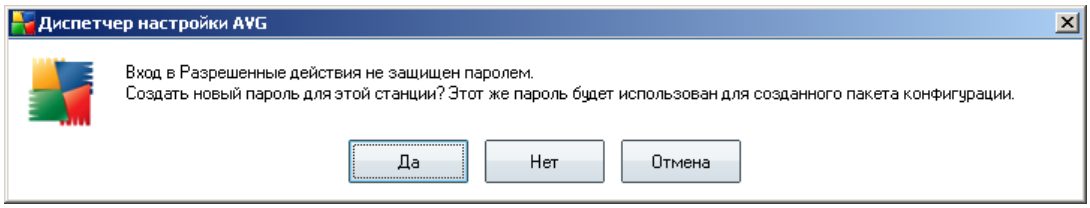
Применить, и файл будет заменен файлом с новыми параметрами.

- ***Применить конфигурацию из файла к программе AVG на данном компьютере***

  Данная кнопка позволяет открыть файл конфигурации AVG (.pck) и применить содержащуюся в нем конфигурацию к локальной версии программы AVG.

- ***Сохранить конфигурацию локальной версии AVG в файл***

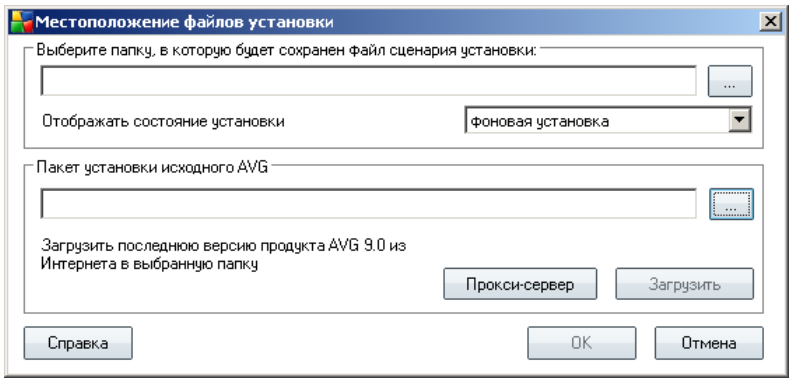
  Данная кнопка позволяет сохранить файл конфигурации локальной версии программы AVG (.pck). Если для разрешенных действий не установлен пароль, может отобразиться следующее диалоговое окно.



  Выберите ответ ***Да***, чтобы установить пароль для доступа разрешенных элементов, а затем указать необходимые сведения и подтвердить выбор. Выберите ответ ***Нет***, чтобы отказаться от создания пароля и перейти к сохранению конфигурации локальной версии программы AVG в файл.

- ***Клонировать установку AVG***

  Данный параметр позволяет создать точную копию локальной установки программы AVG путем создания пакета установки с пользовательскими параметрами. Выберите папку, в которую будет сохранен сценарий установки, чтобы продолжить.



Затем в раскрывающемся меню выберите один из следующих параметров.

- ***Фоновая установка***. Во время процесса установки информация отображаться не будет.
- ***Показывать только состояние процесса установки***. Для установки не потребуется участие пользователя, однако он сможет следить за состоянием процесса установки.
- ***Показывать мастер установки***. Будут отображены все шаги установки, участие пользователя необходимо для подтверждения шагов.

Нажмите кнопку ***Загрузить***, чтобы загрузить последнюю версию пакета установки AVG с веб-сайта AVG в выбранную папку, или поместите пакет установки программы AVG в эту папку вручную.

Нажмите кнопку ***Прокси-сервер***, чтобы определить параметры прокси-сервера, если это требуется для успешного сетевого подключения.

При нажатии кнопки ***OK*** начнется процесс клонирования. Процесс не займет много времени. Также может отобразиться диалоговое окно с запросом на создание пароля для разрешенных элементов (см. выше). По завершении процесса клонирования в выбранной папке появится файл ***AvgSetup.bat***, а также другие файлы установки. Если запустить файл ***AvgSetup.bat***, будет выполнена установка программы AVG в соответствии с описанными выше параметрами.

15. Часто задаваемые вопросы и техническая поддержка

При возникновении любых проблем при работе с программой коммерческого или технического характера см. раздел ***Часто задаваемые вопросы*** веб-сайта AVG (http://www.avg.com).

Если необходимые справочные сведения не найдены, обратитесь в службу технической поддержки по электронной почте. Используйте контактную форму системного меню, доступную в разделе ***Справка/Получить интерактивную справку***.